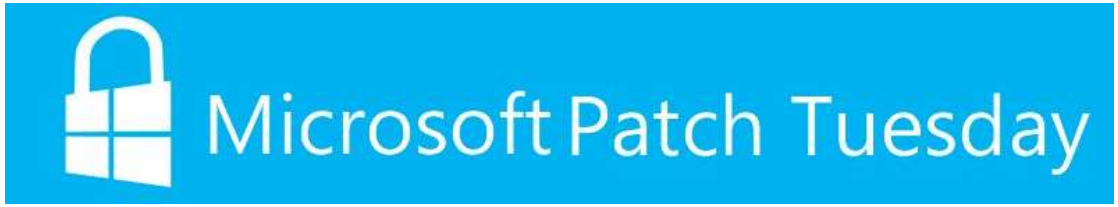
Microsoft's Security Bulletin for May Patches That Fix 111 Security Vulnerabilities

Threat Alert



Overview

Microsoft released the May 2020 security patch on Tuesday that fixes 111 vulnerabilities ranging from simple spoofing attacks to remote code execution in various products, including .NET Core, .NET Framework, Active Directory, Common Log File System Driver, Internet Explorer, Microsoft Dynamics, Microsoft Edge, Microsoft Graphics Component, Microsoft JET Database Engine, Microsoft Office, Microsoft Office SharePoint, Microsoft Scripting Engine, Microsoft Windows, Power BI, Visual Studio, Windows Hyper-V, Windows Kernel, Windows Scripting, Windows Subsystem for Linux, Windows Task Scheduler, and Windows Update Stack.

Description of Critical Vulnerabilities

Microsoft fixed 15 critical vulnerabilities, five of which are described in detail as follows:

- **CVE-2020-1023, CVE-2020-1024, CVE-2020-1069, and CVE-2020–1102**

These are RCE vulnerabilities in the SharePoint. Attackers could exploit these vulnerabilities to execute arbitrary code on a victim machine or server. To successfully exploit the CVE-2020-1069 vulnerability, attackers need to upload a crafted package to the SharePoint server. To exploit the CVE-2020-1023, CVE-2020-1024, and CVE-2020–1102 vulnerabilities, attackers need to trick a user into opening a crafted SharePoint file.

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1023
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1024
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1069
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1102

- **CVE-2020-1062**

This is a memory corruption vulnerability in the Internet Explorer web browser. This vulnerability can be triggered when a user accesses a crafted web page controlled by the attacker. An attacker could exploit this vulnerability to corrupt the memory on the target machine and then execute arbitrary code in the context of the current user via a crafted web page. The security update addresses this vulnerability by modifying how Internet Explorer handles objects in memory.

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1062

Vulnerabilities

The following table lists these vulnerabilities.

Product	CVE ID	CVE Title	**Severity Level**

Microsoft Graphics Component	CVE-2020-1117	Microsoft Color Management Remote Code Execution Vulnerability	Critical
Microsoft Graphics Component	CVE-2020-1153	Microsoft Graphics Components Remote Code Execution Vulnerability	Critical
Microsoft Office SharePoint	CVE-2020-1023	Microsoft SharePoint Remote Code Execution Vulnerability	Critical
Microsoft Office SharePoint	CVE-2020-1024	Microsoft SharePoint Remote Code Execution Vulnerability	Critical
Microsoft Office SharePoint	CVE-2020-1069	Microsoft SharePoint Server Remote Code Execution Vulnerability	Critical
Microsoft Office SharePoint	CVE-2020-1102	Microsoft SharePoint Remote Code Execution Vulnerability	Critical
Microsoft Scripting Engine	CVE-2020-1065	Scripting Engine Memory Corruption Vulnerability	Critical

Microsoft Windows	CVE-2020-1028	Media Foundation Memory Corruption Vulnerability	Critical
Microsoft Windows	CVE-2020-1126	Media Foundation Memory Corruption Vulnerability	Critical
Microsoft Windows	CVE-2020-1136	Media Foundation Memory Corruption Vulnerability	Critical
Visual Studio	CVE-2020-1192	Visual Studio Code Python Extension Remote Code Execution Vulnerability	Critical
Internet Explorer	CVE-2020-1064	MSHTML Engine Remote Code Execution Vulnerability	Critical
Internet Explorer	CVE-2020-1093	VBScript Remote Code Execution Vulnerability	Critical
Microsoft Edge	CVE-2020-1056	Microsoft Edge Privilege Escalation Vulnerability	Critical

Internet Explorer	CVE-2020-1062	Internet Explorer Memory Corruption Vulnerability	Critical
.NET Core	CVE-2020-1108	.NET Core & .NET Framework Denial-of-Service Vulnerability	Important
.NET Core	CVE-2020-1161	ASP.NET Core Denial-of-Service Vulnerability	Important
.NET Framework	CVE-2020-1066	.NET Framework Privilege Escalation Vulnerability	Important
Active Directory	CVE-2020-1055	Microsoft Active Directory Federation Services Cross-Site Scripting Vulnerability	Important
Common Log File System Driver	CVE-2020-1154	Windows Common Log File System Driver Privilege Escalation Vulnerability	Important
Microsoft Dynamics	CVE-2020-1063	Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability	Important

Microsoft Edge	CVE-2020-1059	Microsoft Edge Spoofing Vulnerability	Important
Microsoft Edge	CVE-2020-1096	Microsoft Edge PDF Remote Code Execution Vulnerability	Important
Microsoft Graphics Component	CVE-2020-0963	Windows GDI Information Disclosure Vulnerability	Important
Microsoft Graphics Component	CVE-2020-1054	Win32k Privilege Escalation Vulnerability	Important
Microsoft Graphics Component	CVE-2020-1135	Windows Graphics Component Privilege Escalation Vulnerability	Important
Microsoft Graphics Component	CVE-2020-1140	DirectX Privilege Escalation Vulnerability	Important
Microsoft Graphics Component	CVE-2020-1179	Windows GDI Information Disclosure Vulnerability	Important
Microsoft Graphics Component	CVE-2020-1141	Windows GDI Information Disclosure Vulnerability	Important

Microsoft Graphics Component	CVE-2020-1142	Windows GDI Privilege Escalation Vulnerability	Important
Microsoft Graphics Component	CVE-2020-1145	Windows GDI Information Disclosure Vulnerability	Important
Microsoft JET Database Engine	CVE-2020-1175	Jet Database Engine Remote Code Execution Vulnerability	Important
Microsoft JET Database Engine	CVE-2020-1051	Jet Database Engine Remote Code Execution Vulnerability	Important
Microsoft JET Database Engine	CVE-2020-1174	Jet Database Engine Remote Code Execution Vulnerability	Important
Microsoft JET Database Engine	CVE-2020-1176	Jet Database Engine Remote Code Execution Vulnerability	Important
Microsoft Office	CVE-2020-0901	Microsoft Excel Remote Code Execution Vulnerability	Important
Microsoft Office SharePoint	CVE-2020-1099	Microsoft Office SharePoint XSS Vulnerability	Important

Microsoft Office SharePoint	CVE-2020-1101	Microsoft Office SharePoint XSS Vulnerability	Important
Microsoft Office SharePoint	CVE-2020-1107	Microsoft SharePoint Spoofing Vulnerability	Important
Microsoft Office SharePoint	CVE-2020-1100	Microsoft Office SharePoint XSS Vulnerability	Important
Microsoft Office SharePoint	CVE-2020-1103	Microsoft SharePoint Information Disclosure Vulnerability	Important
Microsoft Office SharePoint	CVE-2020-1104	Microsoft SharePoint Spoofing Vulnerability	Important
Microsoft Office SharePoint	CVE-2020-1105	Microsoft SharePoint Spoofing Vulnerability	Important
Microsoft Office SharePoint	CVE-2020-1106	Microsoft Office SharePoint XSS Vulnerability	Important
Microsoft Windows	CVE-2020-1021	Windows Error Reporting Privilege Escalation Vulnerability	Important

Microsoft Windows	CVE-2020-1010	Microsoft Windows Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1048	Windows Print Spooler Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1071	Windows Remote Access Common Dialog Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1076	Windows Denial-of-Service Vulnerability	Important
Microsoft Windows	CVE-2020-1078	Windows Installer Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1084	Connected User Experiences and Telemetry Service Denial-of-Service Vulnerability	Important
Microsoft Windows	CVE-2020-1116	Windows CSRSS Information Disclosure Vulnerability	Important

Microsoft Windows	CVE-2020-1118	Microsoft Windows Transport Layer Security Denial-of-Service Vulnerability	Important
Microsoft Windows	CVE-2020-1124	Windows State Repository Service Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1134	Windows State Repository Service Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1137	Windows Push Notification Service Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1138	Windows Storage Service Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1143	Win32k Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1144	Windows State Repository Service Privilege Escalation Vulnerability	Important

Microsoft Windows	CVE-2020-1149	Windows Runtime Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1150	Media Foundation Memory Corruption Vulnerability	Important
Microsoft Windows	CVE-2020-1151	Windows Runtime Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1155	Windows Runtime Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1156	Windows Runtime Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1157	Windows Runtime Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1158	Windows Runtime Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1186	Windows State Repository Service Privilege Escalation Vulnerability	Important

Microsoft Windows	CVE-2020-1189	Windows State Repository Service Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1190	Windows State Repository Service Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1067	Windows Remote Code Execution Vulnerability	Important
Microsoft Windows	CVE-2020-1068	Microsoft Windows Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1070	Windows Print Spooler Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1072	Windows Kernel Information Disclosure Vulnerability	Important
Microsoft Windows	CVE-2020-1077	Windows Runtime Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1079	Microsoft Windows Privilege Escalation Vulnerability	Important

Microsoft Windows	CVE-2020-1081	Windows Printer Service Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1082	Windows Error Reporting Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1086	Windows Runtime Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1088	Windows Error Reporting Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1090	Windows Runtime Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1111	Windows Clipboard Service Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1112	Windows Background Intelligent Transfer Service Privilege Escalation Vulnerability	Important

Microsoft Windows	CVE-2020-1121	Windows Clipboard Service Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1123	Connected User Experiences and Telemetry Service Denial-of-Service Vulnerability	Important
Microsoft Windows	CVE-2020-1125	Windows Runtime Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1131	Windows State Repository Service Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1132	Windows Error Reporting Manager Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1139	Windows Runtime Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1164	Windows Runtime Privilege Escalation Vulnerability	Important

Microsoft Windows	CVE-2020-1165	Windows Clipboard Service Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1166	Windows Clipboard Service Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1184	Windows State Repository Service Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1185	Windows State Repository Service Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1187	Windows State Repository Service Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1188	Windows State Repository Service Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2020-1191	Windows State Repository Service Privilege Escalation Vulnerability	Important
Power BI	CVE-2020-1173	Microsoft Power BI Report Server Spoofing Vulnerability	Important

Visual Studio	CVE-2020-1171	Visual Studio Code Python Extension Remote Code Execution Vulnerability	Important
Windows Hyper-V	CVE-2020-0909	Windows Hyper-V Denial-of-Service Vulnerability	Important
Windows Kernel	CVE-2020-1114	Windows Kernel Privilege Escalation Vulnerability	Important
Windows Kernel	CVE-2020-1087	Windows Kernel Privilege Escalation Vulnerability	Important
Windows Scripting	CVE-2020-1061	Microsoft Script Runtime Remote Code Execution Vulnerability	Important
Windows Subsystem for Linux	CVE-2020-1075	Windows Subsystem for Linux Information Disclosure Vulnerability	Important
Windows Task Scheduler	CVE-2020-1113	Windows Task Scheduler Security Feature Bypass Vulnerability	Important

Windows Update Stack	CVE-2020-1110	Windows Update Stack Privilege Escalation Vulnerability	Important
Windows Update Stack	CVE-2020-1109	Windows Update Stack Privilege Escalation Vulnerability	Important
Internet Explorer	CVE-2020-1092	Internet Explorer Memory Corruption Vulnerability	Low
Microsoft Scripting Engine	CVE-2020-1035	VBScript Remote Code Execution Vulnerability	Low
Microsoft Scripting Engine	CVE-2020-1058	VBScript Remote Code Execution Vulnerability	Low
Microsoft Scripting Engine	CVE-2020-1060	VBScript Remote Code Execution Vulnerability	Low
Microsoft Scripting Engine	CVE-2020-1037	Chakra Scripting Engine Memory Corruption Vulnerability	Moderate

Recommended Mitigation Measures

Microsoft has released security updates to fix these issues. Please download and install them as soon as possible.

Appendix

CVE-2020-0901 - Microsoft Excel Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0901 MITRE NVD	**CVE Title:** Microsoft Excel Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Excel. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Excel handles objects in memory. **FAQ:** **What is Microsoft 365 Apps for Enterprise?** Office 365 ProPlus has been renamed to Microsoft 365 Apps for Enterprise. Please see Name change for Office 365 ProPlus for more information. **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-0901						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft 365 Apps for Enterprise for 64-bit Systems	Click to Run Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office 2019 for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution		Base: N/A Temporal:	No

CVE-2020-0901						
					N/A Vector: N/A	
Microsoft Office 2019 for 64-bit editions	Click to Run Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office 2019 for Mac	Release Notes Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Excel 2016 (32-bit edition)	4484338 Security Update	Important	Remote Code Execution	4484273	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 (64-bit edition)	4484338 Security Update	Important	Remote Code Execution	4484273	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 for Mac	Release Notes Security Update	Important	Remote Code Execution	4484273	Base: N/A Temporal: N/A Vector: N/A	No

CVE-2020-0901						
Microsoft Excel 2010 Service Pack 2 (32-bit editions)	4484384 Security Update	Important	Remote Code Execution	4484285	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2010 Service Pack 2 (64-bit editions)	4484384 Security Update	Important	Remote Code Execution	4484285	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 RT Service Pack 1	4484365 Security Update	Important	Remote Code Execution	4484283	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (32-bit editions)	4484365 Security Update	Important	Remote Code Execution	4484283	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (64-bit editions)	4484365 Security Update	Important	Remote Code Execution	4484283	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft 365 Apps for Enterprise for 32-bit Systems	Click to Run Security Update	Important	Remote Code Execution	4484283	Base: N/A Temporal:	No

CVE-2020-0901						
					N/A Vector: N/A	

CVE-2020-0909 - Windows Hyper-V Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0909 MITRE NVD	**CVE Title:** Windows Hyper-V Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when Hyper-V on a Windows Server fails to properly handle specially crafted network packets. To exploit the vulnerability, an attacker would send specially crafted network packets to the Hyper-V Server. The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to properly handle these network packets. **FAQ:** None **Mitigations:** None	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-0909						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Denial of Service	4550922	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0909						
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Denial of Service	4550922	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Denial of Service	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Denial of Service	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Denial of Service	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Denial of Service	4550927	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0909						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Denial of Service	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Denial of Service	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Denial of Service	4550930	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Denial of Service	4550929	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Denial of Service	4550929	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0909						
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Denial of Service	4550929	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Denial of Service	4550964	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Important	Denial of Service	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security	Important	Denial of Service	4550951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0909						
	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Denial of Service	4550951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Denial of Service	4550964	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4556836 Monthly Rollup 4556843 Security Only	Important	Denial of Service	4550964	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0909						
Windows Server 2012	4556840 Monthly Rollup 4556852 Security Only	Important	Denial of Service	4550917	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security Only	Important	Denial of Service	4550917	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security Only	Important	Denial of Service	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0909						
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security Only	Important	Denial of Service	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Denial of Service	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Denial of Service	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0963 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0963 MITRE NVD	**CVE Title:** Windows GDI Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how the Windows GDI component handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is memory layout - the vulnerability allows an attacker to collect information that facilitates predicting addressing of the memory.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-0963						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version	4556807 Security	Important	Information Disclosure	4550922	Base: 5.5 Temporal: 5	Yes

CVE-2020-0963						
1803 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Information Disclosure	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Information Disclosure	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Information Disclosure	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-0963						
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-0963						
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Information Disclosure	4550927	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version	4556812 Security	Important	Information Disclosure	4550927	Base: 5.5 Temporal: 5	Yes

CVE-2020-0963						
1709 for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Information Disclosure	4550927	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-0963						
based Systems						
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Information Disclosure	4550930	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Information Disclosure	4550930	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Information Disclosure	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for	4556813 Security	Important	Information Disclosure	4550929	Base: 5.5 Temporal: 5	Unknown

CVE-2020-0963						
x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2016	4556813 Security Update	Important	Information Disclosure	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Information Disclosure	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 7 for 32-bit Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Information Disclosure	4550964	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 7 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security	Important	Information Disclosure	4550964	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-0963						
	Only					
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Information Disclosure	4550961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Important	Information Disclosure	4550961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4556846 Monthly Rollup	Important	Information Disclosure	4550961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit	4556860 Monthly Rollup	Important	Information Disclosure	4550951	Base: 5.5 Temporal: 5	Unknown

CVE-2020-0963						
Systems Service Pack 2	4556854 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Information Disclosure	4550951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Information Disclosure	4550951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based	4556860 Monthly Rollup 4556854	Important	Information Disclosure	4550951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-0963						
Systems Service Pack 2	Security Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Information Disclosure	4550951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Information Disclosure	4550964	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-	4556836 Monthly Rollup	Important	Information Disclosure	4550964	Base: 5.5 Temporal: 5	Unknown

CVE-2020-0963						
based Systems Service Pack 1	4556843 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4556836 Monthly Rollup 4556843 Security Only	Important	Information Disclosure	4550964	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2012	4556840 Monthly Rollup 4556852 Security Only	Important	Information Disclosure	4550917	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4556840 Monthly Rollup	Important	Information Disclosure	4550917	Base: 5.5 Temporal: 5	Yes

CVE-2020-0963						
(Server Core installation)	4556852 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security Only	Important	Information Disclosure	4550961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security Only	Important	Information Disclosure	4550961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1010 - Microsoft Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1010 MITRE NVD	**CVE Title:** Microsoft Windows Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows Block Level Backup Engine Service (wbengine) that allows file deletion in arbitrary locations. To exploit the vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses the vulnerability by correcting how the Windows Block Level Backup Engine Service handles file operations. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1010						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1010						
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1010						
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1010						
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1010						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1010						
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for 32-bit Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1010						
Windows 7 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1010						
Windows RT 8.1	4556846 Monthly Rollup	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based	4556836 Monthly Rollup 4556843	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1010						
Systems Service Pack 1 (Server Core installation)	Security Only					
Windows Server 2012	4556840 Monthly Rollup 4556852 Security Only	Important	Elevation of Privilege	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security Only	Important	Elevation of Privilege	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4556846 Monthly Rollup 4556853	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1010						
	Security Only					
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1021 - Windows Error Reporting Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1021 MITRE NVD	**CVE Title:** Windows Error Reporting Elevation of Privilege Vulnerability **Description:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files. The vulnerability could allow elevation of privilege if an attacker can successfully exploit it. An attacker who successfully exploited the vulnerability could gain greater access to sensitive information and system functionality. To exploit the vulnerability, an attacker could run a specially crafted application. The security update addresses the vulnerability by correcting the way that WER handles and executes files. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1021						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-	4556807 Security	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7	Yes

CVE-2020-1021						
based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1021						
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1021						
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1021						
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1021						
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1023 - Microsoft SharePoint Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1023 MITRE NVD	**CVE Title:** Microsoft SharePoint Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the SharePoint application pool and the SharePoint server farm account.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Exploitation of this vulnerability requires that a user uploads a specially crafted SharePoint application package to an affected version of SharePoint. The security update addresses the vulnerability by correcting how SharePoint checks the source markup of application packages. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1023						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Enterprise Server 2016	4484336 Security Update	Critical	Remote Code Execution	4484299	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Server 2019	4484332 Security Update	Critical	Remote Code Execution	4484292	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Foundation 2013 Service Pack 1	4484364 Security Update	Critical	Remote Code Execution	4484321	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1024 - Microsoft SharePoint Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1024 MITRE NVD	**CVE Title:** Microsoft SharePoint Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the SharePoint application pool and the SharePoint server farm account. Exploitation of this vulnerability requires that a user uploads a specially crafted SharePoint application package to an affected version of SharePoint. The security update addresses the vulnerability by correcting how SharePoint checks the source markup of application packages. **FAQ:** None **Mitigations:** None **Workarounds:** None	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1024						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Enterprise Server 2016	4484336 Security Update	Critical	Remote Code Execution	4484299	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Server 2019	4484332 Security Update	Critical	Remote Code Execution	4484292	Base: N/A Temporal:	Maybe

CVE-2020-1024						
					N/A Vector: N/A	
Microsoft SharePoint Foundation 2013 Service Pack 1	4484364 Security Update	Critical	Remote Code Execution	4484321	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1028 - Media Foundation Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1028 MITRE NVD	**CVE Title:** Media Foundation Memory Corruption Vulnerability **Description:** A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory. An attacker who successfully exploited the vulnerability could install programs; view, change, or delete data; or create new accounts with full user rights. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit a malicious webpage.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how Windows Media Foundation handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1028						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809	4551853 Security	Critical	Remote Code Execution	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1028						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1028						
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1028						
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1028						
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1035 - VBScript Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1035 MITRE NVD	**CVE Title:** VBScript Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.	Low	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1035						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	4556860 Monthly Rollup 4556798 IE Cumulative	Low	Remote Code Execution	4550905	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556798 IE Cumulative	Low	Remote Code Execution	4550905	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1035						
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1035						
Version 1803 for ARM64-based Systems						
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1035						
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows Server 2019	4551853 Security Update	Low	Remote Code Execution	4549949	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 10 Version 1909 for	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1035						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1035						
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1035						
Version 1709 for ARM64-based Systems						
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1035						
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4556826 Security Update	Important	Remote Code Execution	4550930	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for	4556826 Security Update	Important	Remote Code Execution	4550930	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1035						
x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on	4556813 Security	Low	Remote Code Execution	4550929	Base: 6.4 Temporal: 5.8	Unknown

CVE-2020-1035						
Windows Server 2016	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4556798 IE Cumulative 4556836 Monthly Rollup	Important	Remote Code Execution	4550964	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4556798 IE Cumulative 4556836 Monthly Rollup	Important	Remote Code Execution	4550964	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1035						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4556798 IE Cumulative 4556846 Monthly Rollup	Important	Remote Code Execution	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4556798 IE Cumulative 4556846 Monthly Rollup	Important	Remote Code Execution	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows RT 8.1	4556846 Monthly Rollup	Important	Remote Code Execution	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4556798 IE Cumulative 4556836 Monthly	Low	Remote Code Execution	4550964	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1035						
Server 2008 R2 for x64-based Systems Service Pack 1	Rollup					
Internet Explorer 11 on Windows Server 2012	4556798 IE Cumulative 4556840 Monthly Rollup	Low	Remote Code Execution	4550917	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4556798 IE Cumulative 4556846 Monthly Rollup	Low	Remote Code Execution	4550961	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1037 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1037 MITRE NVD	**CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based). The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge (HTML-based) and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1037						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2020-1037						
ChakraCore	Release Notes Security Update	Critical	Remote Code Execution		Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1037						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1037						
for x64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown
Microsoft Edge (EdgeHTML-based) on Windows Server 2019	4551853 Security Update	Moderate	Remote Code Execution	4549949	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1037						
for 32-bit Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1037						
Version 1709 for 32-bit Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1037						
Windows 10 Version 1903 for 32-bit Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-	4556826 Security	Critical	Remote Code Execution	4550930	Base: 4.2 Temporal: 3.8	Yes

CVE-2020-1037						
based) on Windows 10 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge (EdgeHTML-based) on Windows 10 for x64-based Systems	4556826 Security Update	Critical	Remote Code Execution	4550930	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown
Microsoft Edge (EdgeHTML-based) on	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1037						
Windows 10 Version 1607 for x64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows Server 2016	4556813 Security Update	Moderate	Remote Code Execution	4550929	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1048 - Windows Print Spooler Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1048 MITRE NVD	**CVE Title:** Windows Print Spooler Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system. An attacker who successfully exploited this	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	vulnerability could run arbitrary code with elevated system privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted script or application. The update addresses the vulnerability by correcting how the Windows Print Spooler Component writes to the file system. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1048						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-	4556807 Security	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7	Yes

CVE-2020-1048						
based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1048						
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1048						
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1048						
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1048						
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for 32-bit Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1048						
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4556846 Monthly Rollup	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems	4556860 Monthly Rollup 4556854 Security	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1048						
Service Pack 2	Only					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1048						
	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems	4556836 Monthly Rollup 4556843 Security	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1048						
Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2012	4556840 Monthly Rollup 4556852 Security Only	Important	Elevation of Privilege	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security	Important	Elevation of Privilege	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1048						
	Only					
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1051 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1051 MITRE NVD	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1051						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1051						
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1051						
Windows Server 2019	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1051						
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1051						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Remote Code Execution	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Remote Code Execution	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1051						
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for 32-bit Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1051						
Windows 7 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1051						
Windows RT 8.1	4556846 Monthly Rollup	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for Itanium-Based	4556860 Monthly Rollup 4556854	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1051						
Systems Service Pack 2	Security Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for Itanium-Based	4556836 Monthly Rollup 4556843 Security	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1051						
Systems Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2012	4556840 Monthly Rollup 4556852	Important	Remote Code Execution	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1051						
	Security Only					
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security Only	Important	Remote Code Execution	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security Only	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1051						
	Only					

CVE-2020-1054 - Win32k Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1054 MITRE NVD	**CVE Title:** Win32k Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how the Windows kernel-mode driver handles objects in memory.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1054						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2020-1054						
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1054						
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1054						
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1054						
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1054						
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3	Unknown

CVE-2020-1054						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 7 for 32-bit Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1054						
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4556846 Monthly Rollup	Important	Elevation of Privilege	4550961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: N/A Temporal: N/A Vector: N/A	Unknown
Windows Server 2008 for 32-bit Systems Service Pack	4556860 Monthly Rollup 4556854 Security	Important	Elevation of Privilege	4550951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1054						
2 (Server Core installation)	Only					
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server	4556860 Monthly Rollup 4556854 Security	Important	Elevation of Privilege	4550951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1054						
Core installation)	Only					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack	4556836 Monthly Rollup 4556843 Security	Important	Elevation of Privilege	4550964	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1054						
1 (Server Core installation)	Only					
Windows Server 2012	4556840 Monthly Rollup 4556852 Security Only	Important	Elevation of Privilege	4550917	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security Only	Important	Elevation of Privilege	4550917	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security	Important	Elevation of Privilege	4550961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1054						
	Only					
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1055 - Microsoft Active Directory Federation Services Cross-Site Scripting Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1055 MITRE NVD	**CVE Title:** Microsoft Active Directory Federation Services Cross-Site Scripting Vulnerability **Description:**	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	A cross-site-scripting (XSS) vulnerability exists when Active Directory Federation Services (ADFS) does not properly sanitize user inputs. An un-authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected ADFS server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run scripts in the security context of the current user. This security update addresses the vulnerability by ensuring that ADFS properly sanitizes user inputs. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1055						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Spoofing	4549949	Base: N/A Temporal: N/A Vector: N/A	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Spoofing	4549949	Base: N/A Temporal: N/A Vector: N/A	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Spoofing	4549949	Base: N/A Temporal: N/A Vector: N/A	Unknown
Windows Server 2019	4551853 Security Update	Important	Spoofing	4549949	Base: N/A Temporal: N/A Vector: N/A	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Spoofing	4549949	Base: N/A Temporal: N/A Vector: N/A	Unknown

CVE-2020-1055						
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Spoofing	4549951	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Spoofing	4549951	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Spoofing	4549951	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Spoofing	4549951	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Spoofing	4549951	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Spoofing	4549951	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Spoofing	4549951	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2020-1055						
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Spoofing	4549951	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2020-1056 - Microsoft Edge Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1056 MITRE NVD	**CVE Title:** Microsoft Edge Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft Edge does not properly enforce cross-domain policies, which could allow an attacker to access information from one domain and inject it into another domain. In a web-based attack scenario, an attacker could host a website that is used to attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action. For example, an attacker could trick users into clicking a link that takes them to the attacker's site. An attacker who	Moderate	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	successfully exploited this vulnerability could elevate privileges in affected versions of Microsoft Edge. The security update addresses the vulnerability by helping to ensure that cross-domain policies are properly enforced in Microsoft Edge. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1056						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Critical	Elevation of Privilege	4550922	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Critical	Elevation of Privilege	4550922	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10	4556807 Security Update	Critical	Elevation of Privilege	4550922	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1056						
Version 1803 for ARM64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Critical	Elevation of Privilege	4549949	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Critical	Elevation of Privilege	4549949	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown
Microsoft Edge (EdgeHTML-based) on	4551853 Security Update	Critical	Elevation of Privilege	4549949	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1056						
Windows 10 Version 1809 for ARM64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows Server 2019	4551853 Security Update	Moderate	Elevation of Privilege	4549949	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Critical	Elevation of Privilege	4549951	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10	4556799 Security Update	Critical	Elevation of Privilege	4549951	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1056						
Version 1909 for x64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Critical	Elevation of Privilege	4549951	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Critical	Elevation of Privilege	4550927	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on	4556812 Security Update	Critical	Elevation of Privilege	4550927	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1056						
Windows 10 Version 1709 for x64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Critical	Elevation of Privilege	4550927	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Critical	Elevation of Privilege	4549951	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-	4556799 Security	Critical	Elevation of Privilege	4549951	Base: 5.4 Temporal: 4.9	Yes

CVE-2020-1056						
based) on Windows 10 Version 1903 for x64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Critical	Elevation of Privilege	4549951	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Critical	Elevation of Privilege	4550929	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1056						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Critical	Elevation of Privilege	4550929	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown
Microsoft Edge (EdgeHTML-based) on Windows Server 2016	4556813 Security Update	Moderate	Elevation of Privilege	4550929	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1058 - VBScript Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1058 MITRE NVD	**CVE Title:** VBScript Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.	Low	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1058						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	4556860 Monthly Rollup 4556798 IE Cumulative	Low	Remote Code Execution	4550905	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556798 IE Cumulative	Low	Remote Code Execution	4550905	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1058						
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1058						
Version 1803 for ARM64-based Systems						
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1058						
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows Server 2019	4551853 Security Update	Low	Remote Code Execution	4549949	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 10 Version 1909 for	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1058						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1058						
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1058						
Version 1709 for ARM64-based Systems						
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1058						
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4556826 Security Update	Important	Remote Code Execution	4550930	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for	4556826 Security Update	Important	Remote Code Execution	4550930	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1058						
x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on	4556813 Security	Low	Remote Code Execution	4550929	Base: 6.4 Temporal: 5.8	Unknown

CVE-2020-1058						
Windows Server 2016	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4556798 IE Cumulative 4556836 Monthly Rollup	Important	Remote Code Execution	4550964	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4556798 IE Cumulative 4556836 Monthly Rollup	Important	Remote Code Execution	4550964	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1058						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4556798 IE Cumulative 4556846 Monthly Rollup	Important	Remote Code Execution	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4556798 IE Cumulative 4556846 Monthly Rollup	Important	Remote Code Execution	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows RT 8.1	4556846 Monthly Rollup	Important	Remote Code Execution	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4556798 IE Cumulative 4556836 Monthly	Low	Remote Code Execution	4550964	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1058						
Server 2008 R2 for x64-based Systems Service Pack 1	Rollup					
Internet Explorer 11 on Windows Server 2012	4556798 IE Cumulative 4556840 Monthly Rollup	Low	Remote Code Execution	4550917	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4556798 IE Cumulative 4556846 Monthly Rollup	Low	Remote Code Execution	4550961	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1059 - Microsoft Edge Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1059 MITRE NVD	**CVE Title:** Microsoft Edge Spoofing Vulnerability **Description:** A spoofing vulnerability exists when Microsoft Edge does not properly parse HTTP content. An attacker who successfully exploited this vulnerability could trick a user by redirecting the user to a specially crafted website. The specially crafted website could either spoof content or serve as a pivot to chain an attack with other vulnerabilities in web services. To exploit the vulnerability, the user must click a specially crafted URL. In an email attack scenario, an attacker could send an email message containing the specially crafted URL to the user in an attempt to convince the user to click it. In a web-based attack scenario, an attacker could host a specially crafted website designed to appear as a legitimate website to the user. However, the attacker would have no way to force the user to visit the specially crafted website. The attacker would have to convince the user to visit the specially crafted website, typically by way of enticement in an email or instant message, and then convince the user to interact with content on the website. The update addresses the vulnerability by correcting how Microsoft Edge parses HTTP responses.	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1059						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2020-1059						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Spoofing	4550922	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Spoofing	4550922	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803	4556807 Security Update	Important	Spoofing	4550922	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1059						
for ARM64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Spoofing	4549949	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Unknown
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Spoofing	4549949	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Unknown
Microsoft Edge (EdgeHTML-based) on Windows 10	4551853 Security Update	Important	Spoofing	4549949	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1059						
Version 1809 for ARM64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows Server 2019	4551853 Security Update	Low	Spoofing	4549949	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Unknown
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Spoofing	4549951	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909	4556799 Security Update	Important	Spoofing	4549951	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1059						
for x64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Spoofing	4549951	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Spoofing	4549951	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10	4556799 Security Update	Important	Spoofing	4549951	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1059						
Version 1903 for x64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Spoofing	4549951	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1060 - VBScript Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1060	**CVE Title:** VBScript Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute	Low	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1060						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows Server 2008 for	4556860 Monthly Rollup 4556798 IE Cumulative	Low	Remote Code Execution	4550905	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1060						
32-bit Systems Service Pack 2						
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556798 IE Cumulative	Low	Remote Code Execution	4550905	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1060						
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1060						
10 Version 1809 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1060						
based Systems						
Internet Explorer 11 on Windows Server 2019	4551853 Security Update	Low	Remote Code Execution	4549949	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1060						
1909 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1060						
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1060						
10 Version 1903 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1060						
based Systems						
Internet Explorer 11 on Windows 10 for 32-bit Systems	4556826 Security Update	Important	Remote Code Execution	4550930	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4556826 Security Update	Important	Remote Code Execution	4550930	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1060						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows Server 2016	4556813 Security Update	Low	Remote Code Execution	4550929	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 7 for 32-bit	4556798 IE Cumulative 4556836 Monthly Rollup	Important	Remote Code Execution	4550964	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1060						
Systems Service Pack 1						
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4556798 IE Cumulative 4556836 Monthly Rollup	Important	Remote Code Execution	4550964	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4556798 IE Cumulative 4556846 Monthly Rollup	Important	Remote Code Execution	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4556798 IE Cumulative 4556846 Monthly	Important	Remote Code Execution	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1060						
8.1 for x64-based systems	Rollup					
Internet Explorer 11 on Windows RT 8.1	4556846 Monthly Rollup	Important	Remote Code Execution	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556798 IE Cumulative 4556836 Monthly Rollup	Low	Remote Code Execution	4550964	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows	4556798 IE Cumulative 4556840 Monthly	Low	Remote Code Execution	4550917	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1060						
Server 2012	Rollup					
Internet Explorer 11 on Windows Server 2012 R2	4556798 IE Cumulative 4556846 Monthly Rollup	Low	Remote Code Execution	4550961	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1061 - Microsoft Script Runtime Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1061 MITRE NVD	**CVE Title:** Microsoft Script Runtime Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that the Microsoft Script Runtime handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the Microsoft Script Runtime handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1061						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-	4556807 Security	Important	Remote Code Execution	4550922	Base: 7.5 Temporal: 6.7	Yes

CVE-2020-1061						
based Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1061						
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1061						
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1061						
based Systems						
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1061						
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Remote Code Execution	4550930	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Remote Code Execution	4550930	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1061						
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for 32-bit Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security	Important	Remote Code Execution	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1061						
	Only					
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Important	Remote Code Execution	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4556846 Monthly Rollup	Important	Remote Code Execution	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Remote Code Execution	4550951	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit	4556860 Monthly Rollup	Important	Remote Code Execution	4550951	Base: 6.4 Temporal: 5.8	Unknown

CVE-2020-1061						
Systems Service Pack 2 (Server Core installation)	4556854 Security Only				Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Remote Code Execution	4550951	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Remote Code Execution	4550951	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based	4556860 Monthly Rollup 4556854	Important	Remote Code Execution	4550951	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1061						
Systems Service Pack 2 (Server Core installation)	Security Only					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-	4556836 Monthly Rollup	Important	Remote Code Execution	4550964	Base: 6.4 Temporal: 5.8	Unknown

CVE-2020-1061						
based Systems Service Pack 1 (Server Core installation)	4556843 Security Only				Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2012	4556840 Monthly Rollup 4556852 Security Only	Important	Remote Code Execution	4550917	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security Only	Important	Remote Code Execution	4550917	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4556846 Monthly Rollup	Important	Remote Code Execution	4550961	Base: 6.4 Temporal: 5.8	Yes

CVE-2020-1061						
	4556853 Security Only				Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security Only	Important	Remote Code Execution	4550961	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1062 - Internet Explorer Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1062	**CVE Title:** Internet Explorer Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, the attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. An attacker could host a specially crafted website designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. The attacker could also take advantage of compromised websites, or websites that accept or host user-provided content or advertisements, by adding specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action, typically by an enticement in an email or instant message, or by getting the user to open an attachment sent through email. The security update addresses the vulnerability by modifying how Internet Explorer handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1062						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows Server 2008 for	4556860 Monthly Rollup 4556798 IE Cumulative	Moderate	Remote Code Execution	4550905	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1062						
32-bit Systems Service Pack 2						
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556798 IE Cumulative	Moderate	Remote Code Execution	4550905	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1062						
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1809 for	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1062						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows	4551853 Security Update	Moderate	Remote Code Execution	4549949	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1062						
Server 2019						
Internet Explorer 11 on Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1062						
1909 for ARM64-based Systems						
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4556812 Security	Critical	Remote Code Execution	4550927	Base: 7.5 Temporal: 6.7	Yes

CVE-2020-1062						
Windows 10 Version 1709 for ARM64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1062						
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4556826 Security Update	Critical	Remote Code Execution	4550930	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4556826 Security Update	Critical	Remote Code Execution	4550930	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1062						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows Server 2016	4556813 Security Update	Moderate	Remote Code Execution	4550929	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1062						
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4556798 IE Cumulative 4556836 Monthly Rollup	Critical	Remote Code Execution	4550964	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4556798 IE Cumulative 4556836 Monthly Rollup	Critical	Remote Code Execution	4550964	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 8.1 for 32-	4556798 IE Cumulative 4556846 Monthly	Critical	Remote Code Execution	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1062						
bit systems	Rollup					
Internet Explorer 11 on Windows 8.1 for x64-based systems	4556798 IE Cumulative 4556846 Monthly Rollup	Critical	Remote Code Execution	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows RT 8.1	4556846 Monthly Rollup	Critical	Remote Code Execution	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems	4556798 IE Cumulative 4556836 Monthly Rollup	Moderate	Remote Code Execution	4550964	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1062						
Service Pack 1						
Internet Explorer 11 on Windows Server 2012	4556798 IE Cumulative 4556840 Monthly Rollup	Moderate	Remote Code Execution	4550917	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4556798 IE Cumulative 4556846 Monthly Rollup	Moderate	Remote Code Execution	4550961	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1063 - Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1063 MITRE NVD	**CVE Title:** Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability **Description:** A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected Dynamics server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current authenticated user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions within Dynamics Server on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that Dynamics Server properly sanitizes web requests.	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1063						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2020-1063						
Microsoft Dynamics 365 (on-premises) version 8.2	4551998 Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Dynamics 365 (on-premises) version 9.0	4552002 Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1064 - MSHTML Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1064 MITRE NVD	**CVE Title:** MSHTML Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that the MSHTML engine improperly validates input. An attacker could execute arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	In a HTML editing attack scenario, an attacker could trick a user into editing a specially crafted file that is designed to exploit the vulnerability. The security update addresses the vulnerability by modifying how MSHTML engine validates input. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1064						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	4556860 Monthly Rollup 4556798 IE Cumulative	Moderate	Remote Code Execution	4550905	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556798 IE Cumulative	Moderate	Remote Code Execution	4550905	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1064						
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1064						
based Systems						
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 10 Version	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1064						
1809 for ARM64-based Systems						
Internet Explorer 11 on Windows Server 2019	4551853 Security Update	Moderate	Remote Code Execution	4549949	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1064						
1909 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4556812 Security	Critical	Remote Code Execution	4550927	Base: 7.5 Temporal: 6.7	Yes

CVE-2020-1064						
Windows 10 Version 1709 for x64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1064						
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for 32-	4556826 Security Update	Critical	Remote Code Execution	4550930	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1064						
bit Systems						
Internet Explorer 11 on Windows 10 for x64-based Systems	4556826 Security Update	Critical	Remote Code Execution	4550930	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 10 Version 1607 for	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1064						
x64-based Systems						
Internet Explorer 11 on Windows Server 2016	4556813 Security Update	Moderate	Remote Code Execution	4550929	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4556798 IE Cumulative 4556836 Monthly Rollup	Critical	Remote Code Execution	4550964	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 7 for x64-based	4556798 IE Cumulative 4556836 Monthly Rollup	Critical	Remote Code Execution	4550964	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1064						
Systems Service Pack 1						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4556798 IE Cumulative 4556846 Monthly Rollup	Critical	Remote Code Execution	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4556798 IE Cumulative 4556846 Monthly Rollup	Critical	Remote Code Execution	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows RT 8.1	4556846 Monthly Rollup	Critical	Remote Code Execution	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1064						
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556798 IE Cumulative 4556836 Monthly Rollup	Moderate	Remote Code Execution	4550964	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows Server 2012	4556798 IE Cumulative 4556840 Monthly Rollup	Moderate	Remote Code Execution	4550917	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4556798 IE Cumulative 4556846 Monthly Rollup	Moderate	Remote Code Execution	4550961	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1065 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1065 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how the ChakraCore scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1065						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
ChakraCore	Release Notes Security Update	Critical	Remote Code Execution		Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2020-1065						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1065						
for ARM64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown
Microsoft Edge (EdgeHTML-based) on Windows 10	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1065						
Version 1809 for ARM64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows Server 2019	4551853 Security Update	Moderate	Remote Code Execution	4549949	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1065						
for x64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1065						
Version 1903 for x64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1066 - .NET Framework Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1066 MITRE NVD	**CVE Title:** .NET Framework Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in .NET Framework which could allow an attacker to elevate their privilege level.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, an attacker would first have to access the local machine, and then run a malicious program. The update addresses the vulnerability by correcting how .NET Framework activates COM objects. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1066						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4556402 Monthly Rollup 4556406 Security Only	Important	Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2	4556402 Monthly Rollup 4556406 Security Only	Important	Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2	4556402 Monthly Rollup 4556406 Security Only	Important	Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows 7 for 32-bit Systems Service Pack 1	4556399 Monthly Rollup	Important	Elevation of Privilege		Base: N/A Temporal:	Maybe

CVE-2020-1066						
	4556403 Security Only				N/A Vector: N/A	
Microsoft .NET Framework 3.5.1 on Windows 7 for x64-based Systems Service Pack 1	4556399 Monthly Rollup 4556403 Security Only	Important	Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4556399 Monthly Rollup 4556403 Security Only	Important	Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556399 Monthly Rollup 4556403 Security Only	Important	Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1066						
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4556399 Monthly Rollup 4556403 Security Only	Important	Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1067 - Windows Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1067 MITRE NVD	**CVE Title:** Windows Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that Windows handles objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary code with elevated permissions on a target system. To exploit the vulnerability, an attacker who has a domain user account could create a specially crafted request, causing Windows to execute arbitrary code with elevated permissions.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how Windows handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1067						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809	4551853 Security	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1067						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1067						
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1067						
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1067						
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Remote Code Execution	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Remote Code Execution	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security	Important	Remote Code Execution	4550929	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1067						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 7 for 32-bit Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1067						
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4556846 Monthly Rollup	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack	4556860 Monthly Rollup 4556854 Security	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1067						
2 (Server Core installation)	Only					
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server	4556860 Monthly Rollup 4556854 Security	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1067						
Core installation)	Only					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack	4556836 Monthly Rollup 4556843 Security	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1067						
1 (Server Core installation)	Only					
Windows Server 2012	4556840 Monthly Rollup 4556852 Security Only	Important	Remote Code Execution	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security Only	Important	Remote Code Execution	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1067						
	Only					
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security Only	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1068 - Microsoft Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1068 MITRE NVD	**CVE Title:** Microsoft Windows Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows Media Service that allows file creation in arbitrary locations.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses the vulnerability by correcting how the Windows Media Service handles file creation. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1068						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1068						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1068						
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1068						
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1068						
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1068						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	

CVE-2020-1069 - Microsoft SharePoint Server Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1069 MITRE NVD	**CVE Title:** Microsoft SharePoint Server Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft SharePoint Server when it fails to properly identify and filter unsafe ASP.Net web controls. An authenticated attacker who successfully exploited the vulnerability could use a specially crafted page to perform actions in the security context of the SharePoint application pool process. To exploit the vulnerability, an authenticated user must create and invoke a specially crafted page on an affected version of Microsoft SharePoint Server. The security update addresses the vulnerability by correcting how Microsoft SharePoint Server handles processing of created content.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1069						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2020-1069						
Microsoft SharePoint Enterprise Server 2016	4484336 Security Update	Critical	Remote Code Execution	4484299	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Server 2019	4484332 Security Update	Critical	Remote Code Execution	4484292	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Foundation 2013 Service Pack 1	4484364 Security Update	Critical	Remote Code Execution	4484321	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1070 - Windows Print Spooler Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1070	**CVE Title:** Windows Print Spooler Elevation of Privilege Vulnerability **Description:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system. An attacker who successfully exploited this vulnerability could run arbitrary code with elevated system privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted script or application. The update addresses the vulnerability by correcting how the Windows Print Spooler Component writes to the file system. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1070						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-	4556807 Security	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7	Yes

CVE-2020-1070						
based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1070						
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1070						
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1070						
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1070						
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for 32-bit Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1070						
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4556846 Monthly Rollup	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems	4556860 Monthly Rollup 4556854 Security	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1070						
Service Pack 2	Only					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1070						
	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems	4556836 Monthly Rollup 4556843 Security	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1070						
Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2012	4556840 Monthly Rollup 4556852 Security Only	Important	Elevation of Privilege	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security	Important	Elevation of Privilege	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1070						
	Only					
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1071 - Windows Remote Access Common Dialog Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1071 MITRE NVD	**CVE Title:** Windows Remote Access Common Dialog Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Windows improperly handles errors tied to Remote Access Common Dialog. An attacker who successfully exploited the vulnerability could run arbitrary code with elevated privileges. To exploit this vulnerability an attacker would need to physically access the booted machine to reach the logon screen. An attacker could then exploit the vulnerability and take control of an affected system. The update addresses the vulnerability by correcting how the Windows handles errors tied to Remote Access Common Dialog. **FAQ:** None **Mitigations:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1071						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1071						
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1071						
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1071						
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1071						
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1071						
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for 32-bit Systems	4556836 Monthly Rollup	Important	Elevation of Privilege	4550964	Base: 6.8 Temporal: 6.1	Unknown

CVE-2020-1071						
Service Pack 1	4556843 Security Only				Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 7 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security	Important	Elevation of Privilege	4550961	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1071						
	Only					
Windows RT 8.1	4556846 Monthly Rollup	Important	Elevation of Privilege	4550961	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1071						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2012	4556840 Monthly Rollup 4556852 Security Only	Important	Elevation of Privilege	4550917	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security Only	Important	Elevation of Privilege	4550917	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1071						
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1072 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1072 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system. The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The type of information that could be disclosed if an attacker successfully exploited this vulnerability is the contents of Kernel memory. An attacker could read the contents of Kernel memory from a user mode process. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1072						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Information Disclosure	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Information Disclosure	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Information Disclosure	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Information Disclosure	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1072						
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1072						
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version	4556812 Security	Important	Information Disclosure	4550927	Base: 5.5 Temporal: 5	Yes

CVE-2020-1072						
1709 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Information Disclosure	4550927	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Information Disclosure	4550927	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1072						
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Information Disclosure	4550930	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Information Disclosure	4550930	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Information Disclosure	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1072						
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Information Disclosure	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Information Disclosure	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Information Disclosure	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 7 for 32-bit Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Information Disclosure	4550964	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 7 for x64-based	4556836 Monthly Rollup	Important	Information Disclosure	4550964	Base: 5.5 Temporal: 5	Unknown

CVE-2020-1072						
Systems Service Pack 1	4556843 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Information Disclosure	4550961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Important	Information Disclosure	4550961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4556846 Monthly Rollup	Important	Information Disclosure	4550961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1072						
Windows Server 2008 for 32-bit Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Information Disclosure	4550951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Information Disclosure	4550951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Information Disclosure	4550951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1072						
Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Information Disclosure	4550951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Information Disclosure	4550951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for Itanium-Based Systems	4556836 Monthly Rollup 4556843 Security Only	Important	Information Disclosure	4550964	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1072						
Service Pack 1						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Information Disclosure	4550964	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4556836 Monthly Rollup 4556843 Security Only	Important	Information Disclosure	4550964	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2012	4556840 Monthly Rollup 4556852 Security	Important	Information Disclosure	4550917	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1072						
	Only					
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security Only	Important	Information Disclosure	4550917	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security Only	Important	Information Disclosure	4550961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security Only	Important	Information Disclosure	4550961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1075 - Windows Subsystem for Linux Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1075 MITRE NVD	**CVE Title:** Windows Subsystem for Linux Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Windows Subsystem for Linux improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system. A attacker could exploit this vulnerability by running a specially crafted application. The update addresses the vulnerability by correcting how Windows Subsystem for Linux handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is the contents of Kernel memory. An attacker could read the contents of Kernel memory from a user mode process.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1075						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version	4556807 Security	Important	Information Disclosure	4550922	Base: 5.5 Temporal: 5	Yes

CVE-2020-1075						
1803 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Information Disclosure	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Information Disclosure	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Information Disclosure	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version	4551853 Security	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5	Unknown

CVE-2020-1075						
1809 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1075						
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1075						
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1076 - Windows Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1076 MITRE NVD	**CVE Title:** Windows Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when Windows improperly handles objects in memory. An attacker who successfully exploited the vulnerability could cause a target system to stop responding. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to cause a target system to stop responding. The update addresses the vulnerability by correcting how Windows handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1076						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Denial of Service	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803	4556807 Security	Important	Denial of Service	4550922	Base: 5.5 Temporal: 5	Yes

CVE-2020-1076						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Denial of Service	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Denial of Service	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Denial of Service	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Denial of Service	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Denial of Service	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1076						
Windows Server 2019	4551853 Security Update	Important	Denial of Service	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Denial of Service	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Denial of Service	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Denial of Service	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Denial of Service	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909	4556799 Security	Important	Denial of Service	4549951	Base: 5.5 Temporal: 5	Yes

CVE-2020-1076						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Denial of Service	4550927	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Denial of Service	4550927	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Denial of Service	4550927	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Denial of Service	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Denial of Service	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1076						
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Denial of Service	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Denial of Service	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Denial of Service	4550930	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Denial of Service	4550930	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Denial of Service	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1076						
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Denial of Service	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Denial of Service	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Denial of Service	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Denial of Service	4550961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853	Important	Denial of Service	4550961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1076						
	Security Only					
Windows RT 8.1	4556846 Monthly Rollup	Important	Denial of Service	4550961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4556840 Monthly Rollup 4556852 Security Only	Important	Denial of Service	4550917	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security Only	Important	Denial of Service	4550917	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1076						
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security Only	Important	Denial of Service	4550961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security Only	Important	Denial of Service	4550961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1077 - Windows Runtime Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1077	**CVE Title:** Windows Runtime Elevation of Privilege Vulnerability **Description:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows Runtime handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1077						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-	4556807 Security	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7	Yes

CVE-2020-1077						
based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1077						
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1077						
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1077						
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1078 - Windows Installer Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1078 MITRE NVD	**CVE Title:** Windows Installer Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations. To exploit the vulnerability, an attacker would require unprivileged execution on the victim system. After successfully exploiting the vulnerability, an attacker could run arbitrary code with elevated privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by correcting the way Windows Installer handles certain filesystem operations. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1078						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803	4556807 Security	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7	Yes

CVE-2020-1078						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1078						
based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1078						
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1078						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1078						
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for 32-bit Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1078						
Windows 7 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1078						
Windows RT 8.1	4556846 Monthly Rollup	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for Itanium-Based	4556860 Monthly Rollup 4556854	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1078						
Systems Service Pack 2	Security Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for Itanium-Based	4556836 Monthly Rollup 4556843 Security	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1078						
Systems Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2012	4556840 Monthly Rollup 4556852	Important	Elevation of Privilege	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1078						
	Security Only					
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security Only	Important	Elevation of Privilege	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1078						
	Only					

CVE-2020-1079 - Microsoft Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1079 MITRE NVD	**CVE Title:** Microsoft Windows Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application to take control of an affected system. The update addresses the vulnerability by correcting how the Windows handles objects in memory. **FAQ:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1079						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2020-1079						
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1079						
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1079						
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1079						
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1079						
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1079						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4556846 Monthly Rollup	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4556840 Monthly Rollup	Important	Elevation of Privilege	4550917	Base: 7.8 Temporal: 7	Yes

CVE-2020-1079						
	4556852 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security Only	Important	Elevation of Privilege	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1079						
	Only					

CVE-2020-1081 - Windows Printer Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1081 MITRE NVD	**CVE Title:** Windows Printer Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows Printer Service improperly validates file paths while loading printer drivers. An authenticated attacker who successfully exploited this vulnerability could run arbitrary code with elevated system privileges. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how the Windows Printer Service validates file paths.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1081						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2020-1081						
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1081						
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1081						
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1081						
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1081						
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1081						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 7 for 32-bit Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1081						
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4556846 Monthly Rollup	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack	4556860 Monthly Rollup 4556854 Security	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1081						
2 (Server Core installation)	Only					
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server	4556860 Monthly Rollup 4556854 Security	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1081						
Core installation)	Only					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack	4556836 Monthly Rollup 4556843 Security	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1081						
1 (Server Core installation)	Only					
Windows Server 2012	4556840 Monthly Rollup 4556852 Security Only	Important	Elevation of Privilege	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security Only	Important	Elevation of Privilege	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1081						
	Only					
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1082 - Windows Error Reporting Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1082 MITRE NVD	**CVE Title:** Windows Error Reporting Elevation of Privilege Vulnerability **Description:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files. The vulnerability could allow elevation of privilege if an attacker can successfully exploit it. An attacker who successfully exploited the vulnerability could gain greater access to sensitive information and system functionality. To exploit the vulnerability, an attacker could run a specially crafted application. The security update addresses the vulnerability by correcting the way that WER handles and executes files. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1082						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-	4556807 Security	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7	Yes

CVE-2020-1082						
based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1082						
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1082						
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1082						
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1082						
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1084 - Connected User Experiences and Telemetry Service Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1084 MITRE NVD	**CVE Title:** Connected User Experiences and Telemetry Service Denial of Service Vulnerability **Description:**	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	A Denial Of Service vulnerability exists when Connected User Experiences and Telemetry Service fails to validate certain function values. An attacker who successfully exploited this vulnerability could deny dependent security feature functionality. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the Connected User Experiences and Telemetry Service validates certain function values. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1084						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Denial of Service	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Denial of Service	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Denial of Service	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803	4556807 Security	Important	Denial of Service	4550922	Base: 5.5 Temporal: 5	Yes

CVE-2020-1084						
for ARM64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Denial of Service	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Denial of Service	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Denial of Service	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Denial of Service	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Denial of Service	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1084						
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Denial of Service	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Denial of Service	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Denial of Service	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Denial of Service	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Denial of Service	4550927	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1084						
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Denial of Service	4550927	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Denial of Service	4550927	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Denial of Service	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Denial of Service	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Denial of Service	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903	4556799 Security	Important	Denial of Service	4549951	Base: 5.5 Temporal: 5	Yes

CVE-2020-1084						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Denial of Service	4550930	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Denial of Service	4550930	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Denial of Service	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Denial of Service	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Denial of Service	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1084						
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Denial of Service	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1086 - Windows Runtime Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1086 MITRE NVD	**CVE Title:** Windows Runtime Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows Runtime handles objects in memory. **FAQ:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1086						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803	4556807 Security	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7	Yes

CVE-2020-1086						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1086						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1086						
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1086						
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1086						
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1087 - Windows Kernel Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1087 MITRE NVD	**CVE Title:** Windows Kernel Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application. The security update addresses the vulnerability by ensuring the Windows Kernel properly handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1087						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1087						
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1087						
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1087						
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1087						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1088 - Windows Error Reporting Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1088 MITRE NVD	**CVE Title:** Windows Error Reporting Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files. The vulnerability could allow elevation of privilege if an attacker can successfully exploit it. An attacker who successfully exploited the vulnerability could gain greater access to sensitive information and system functionality. To exploit the vulnerability, an attacker could run a specially crafted application. The security update addresses the vulnerability by correcting the way that WER handles and executes files. **FAQ:** None **Mitigations:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1088						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1088						
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1088						
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1088						
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1088						
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1088						
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1090 - Windows Runtime Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1090 MITRE NVD	**CVE Title:** Windows Runtime Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows Runtime handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1090						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1090						
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1090						
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1090						
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1090						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1090						
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1092 - Internet Explorer Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1092 MITRE NVD	**CVE Title:** Internet Explorer Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, the attacker could take control of an affected system. An attacker	Low	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	could then install programs; view, change, or delete data; or create new accounts with full user rights. An attacker could host a specially crafted website designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. The attacker could also take advantage of compromised websites, or websites that accept or host user-provided content or advertisements, by adding specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action, typically by an enticement in an email or instant message, or by getting the user to open an attachment sent through email. The security update addresses the vulnerability by modifying how Internet Explorer handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1092						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems	4556860 Monthly Rollup 4556798 IE Cumulative	Low	Remote Code Execution	4550905	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1092						
Service Pack 2						
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556798 IE Cumulative	Low	Remote Code Execution	4550905	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1092						
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1092						
10 Version 1809 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1092						
based Systems						
Internet Explorer 11 on Windows Server 2019	4551853 Security Update	Low	Remote Code Execution	4549949	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1092						
1909 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1092						
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1092						
10 Version 1903 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1092						
based Systems						
Internet Explorer 11 on Windows 10 for 32-bit Systems	4556826 Security Update	Important	Remote Code Execution	4550930	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4556826 Security Update	Important	Remote Code Execution	4550930	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1092						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows Server 2016	4556813 Security Update	Low	Remote Code Execution	4550929	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 7 for 32-bit	4556798 IE Cumulative 4556836 Monthly Rollup	Important	Remote Code Execution	4550964	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1092						
Systems Service Pack 1						
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4556798 IE Cumulative 4556836 Monthly Rollup	Important	Remote Code Execution	4550964	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4556798 IE Cumulative 4556846 Monthly Rollup	Important	Remote Code Execution	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4556798 IE Cumulative 4556846 Monthly	Important	Remote Code Execution	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1092						
8.1 for x64-based systems	Rollup					
Internet Explorer 11 on Windows RT 8.1	4556846 Monthly Rollup	Important	Remote Code Execution	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556798 IE Cumulative 4556836 Monthly Rollup	Low	Remote Code Execution	4550964	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows	4556798 IE Cumulative 4556840 Monthly	Low	Remote Code Execution	4550917	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1092						
Server 2012	Rollup					
Internet Explorer 11 on Windows Server 2012 R2	4556798 IE Cumulative 4556846 Monthly Rollup	Low	Remote Code Execution	4550961	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1093 - VBScript Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1093 MITRE NVD	**CVE Title:** VBScript Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1093						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems	4556860 Monthly Rollup 4556798 IE Cumulative	Moderate	Remote Code Execution	4550905	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1093						
Service Pack 2						
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556798 IE Cumulative	Moderate	Remote Code Execution	4550905	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4556807 Security	Critical	Remote Code Execution	4550922	Base: 7.5 Temporal: 6.7	Yes

CVE-2020-1093						
Windows 10 Version 1803 for x64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1093						
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows Server 2019	4551853 Security Update	Moderate	Remote Code Execution	4549949	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1093						
Internet Explorer 11 on Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1909 for ARM64-	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1093						
based Systems						
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1093						
1709 for ARM64-based Systems						
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4556799 Security	Critical	Remote Code Execution	4549951	Base: 7.5 Temporal: 6.7	Yes

CVE-2020-1093						
Windows 10 Version 1903 for ARM64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 for 32-bit Systems	4556826 Security Update	Critical	Remote Code Execution	4550930	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4556826 Security Update	Critical	Remote Code Execution	4550930	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4556813 Security	Critical	Remote Code Execution	4550929	Base: 7.5 Temporal: 6.7	Unknown

CVE-2020-1093						
Windows 10 Version 1607 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows Server 2016	4556813 Security Update	Moderate	Remote Code Execution	4550929	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows	4556798 IE Cumulative 4556836 Monthly	Critical	Remote Code Execution	4550964	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1093						
7 for 32-bit Systems Service Pack 1	Rollup					
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4556798 IE Cumulative 4556836 Monthly Rollup	Critical	Remote Code Execution	4550964	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4556798 IE Cumulative 4556846 Monthly Rollup	Critical	Remote Code Execution	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1093						
Internet Explorer 11 on Windows 8.1 for x64-based systems	4556798 IE Cumulative 4556846 Monthly Rollup	Critical	Remote Code Execution	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows RT 8.1	4556846 Monthly Rollup	Critical	Remote Code Execution	4550961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556798 IE Cumulative 4556836 Monthly Rollup	Moderate	Remote Code Execution	4550964	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1093						
Internet Explorer 11 on Windows Server 2012	4556798 IE Cumulative 4556840 Monthly Rollup	Moderate	Remote Code Execution	4550917	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4556798 IE Cumulative 4556846 Monthly Rollup	Moderate	Remote Code Execution	4550961	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1096 - Microsoft Edge PDF Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1096	**CVE Title:** Microsoft Edge PDF Remote Code Execution Vulnerability **Description:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A remote code execution vulnerability exists when Microsoft Edge PDF Reader improperly handles objects in memory. The vulnerability could corrupt memory in such a way that enables an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit the vulnerability, in a web-based attack scenario, an attacker could host a website that contains malicious PDF content. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted PDF content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site. The security update addresses the vulnerability by modifying how Microsoft Edge PDF Reader handles objects in memory. **FAQ:** None **Mitigations:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1096						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge (EdgeHTML-based) on Windows 10	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1096						
Version 1803 for 32-bit Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1096						
Windows 10 Version 1809 for 32-bit Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown
Microsoft Edge (EdgeHTML-	4551853 Security	Low	Remote Code Execution	4549949	Base: 4.2 Temporal: 3.8	Unknown

CVE-2020-1096						
based) on Windows Server 2019	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1096						
Windows 10 Version 1909 for ARM64-based Systems						
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge (EdgeHTML-	4556799 Security	Important	Remote Code Execution	4549951	Base: 4.2 Temporal: 3.8	Yes

CVE-2020-1096						
based) on Windows 10 Version 1903 for ARM64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	

CVE-2020-1099 - Microsoft Office SharePoint XSS Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1099 MITRE NVD	**CVE Title:** Microsoft Office SharePoint XSS Vulnerability **Description:** A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1099						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Enterprise Server 2016	4484336 Security Update	Important	Spoofing	4484299	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Server 2019	4484332 Security Update	Important	Spoofing	4484292	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1100 - Microsoft Office SharePoint XSS Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1100 MITRE NVD	**CVE Title:** Microsoft Office SharePoint XSS Vulnerability **Description:** A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server.	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1100						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Enterprise Server 2016	4484336 Security Update	Important	Spoofing	4484299	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2013 Service Pack 1	4484352 Security Update	Important	Spoofing	4484308	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Server 2019	4484332 Security Update	Important	Spoofing	4484292	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Server 2010 Service Pack 2	4484383 Security Update	Important	Spoofing	4484297	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1101 - Microsoft Office SharePoint XSS Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1101 MITRE NVD	**CVE Title:** Microsoft Office SharePoint XSS Vulnerability **Description:** A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:** None **Mitigations:**	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1101						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Enterprise Server 2016	4484336 Security Update	Important	Spoofing	4484299	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1101						
Microsoft SharePoint Server 2019	4484332 Security Update	Important	Spoofing	4484292	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Foundation 2013 Service Pack 1	4484364 Security Update	Important	Spoofing	4484321	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1102 - Microsoft SharePoint Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1102 MITRE NVD	**CVE Title:** Microsoft SharePoint Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the SharePoint application pool and the SharePoint server farm account. Exploitation of this vulnerability requires that a user uploads a specially crafted SharePoint application package to an affected version of SharePoint.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how SharePoint checks the source markup of application packages. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1102						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Enterprise Server 2016	4484336 Security Update	Critical	Remote Code Execution	4484299	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Server 2019	4484332 Security Update	Critical	Remote Code Execution	4484292	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1103 - Microsoft SharePoint Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1103 MITRE NVD	**CVE Title:** Microsoft SharePoint Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists where certain modes of the search function in Microsoft SharePoint Server are vulnerable to cross-site search attacks (a variant of cross-site request forgery, CSRF). When users are simultaneously logged in to Microsoft SharePoint Server and visit a malicious web page, the attacker can, through standard browser functionality, induce the browser to invoke	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	search queries as the logged in user. While the attacker canâ€™t access the search results or documents as such, the attacker can determine whether the query did return results or not, and thus by issuing targeted queries discover facts about documents that are searchable for the logged-in user. The security update addresses the vulnerability by running the search queries in a way that doesnâ€™t expose them to this browser vulnerability. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is unauthorized file system access - reading from the file system. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1103						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Enterprise Server 2016	4484336 Security Update	Important	Information Disclosure	4484299	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Server 2019	4484332 Security Update	Important	Information Disclosure	4484292	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1103						
Microsoft SharePoint Foundation 2013 Service Pack 1	4484364 Security Update	Important	Information Disclosure	4484321	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1104 - Microsoft SharePoint Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1104 MITRE NVD	**CVE Title:** Microsoft SharePoint Spoofing Vulnerability **Description:** A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user.	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1104						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Enterprise Server 2016	4484336 Security Update	Important	Spoofing	4484299	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Server 2019	4484332 Security Update	Important	Spoofing	4484292	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Foundation 2013 Service Pack 1	4484364 Security Update	Important	Spoofing	4484321	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1105 - Microsoft SharePoint Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1105	**CVE Title:** Microsoft SharePoint Spoofing Vulnerability **Description:**	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1105						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Enterprise Server 2016	4484336 Security Update	Important	Spoofing	4484299	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Foundation 2013 Service Pack 1	4484364 Security Update	Important	Spoofing	4484321	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1106 - Microsoft Office SharePoint XSS Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1106 MITRE NVD	**CVE Title:** Microsoft Office SharePoint XSS Vulnerability **Description:** A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:** None **Mitigations:**	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1106						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Enterprise Server 2016	4484336 Security Update	Important	Spoofing	4484299	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1106						
Microsoft SharePoint Server 2019	4484332 Security Update	Important	Spoofing	4484292	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Foundation 2013 Service Pack 1	4484364 Security Update	Important	Spoofing	4484321	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1107 - Microsoft SharePoint Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1107 MITRE NVD	**CVE Title:** Microsoft SharePoint Spoofing Vulnerability **Description:** A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1107						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Enterprise Server 2016	4484336 Security Update	Important	Spoofing	4484299	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2013 Service Pack 1	4484352 Security Update	Important	Spoofing	4484308	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Server 2019	4484332 Security Update	Important	Spoofing	4484292	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Foundation 2013 Service Pack 1	4484364 Security Update	Important	Spoofing	4484321	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1108 - .NET Core & .NET Framework Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1108 MITRE NVD	**CVE Title:** .NET Core & .NET Framework Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when .NET Core or .NET Framework improperly handles web requests. An attacker who successfully exploited this vulnerability could cause a denial of service against a .NET Core or .NET Framework web application. The vulnerability can be exploited remotely, without authentication. A remote unauthenticated attacker could exploit this vulnerability by issuing specially crafted requests to the .NET Core or .NET Framework application. The update addresses the vulnerability by correcting how the .NET Core or .NET Framework web application handles web requests. **FAQ:** None **Mitigations:**	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1108						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
.NET Core 3.1	Release Notes Security Update	Important	Denial of Service		Base: N/A Temporal: N/A	Maybe

CVE-2020-1108						
					Vector: N/A	
.NET Core 2.1	Release Notes Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Visual Studio 2017 version 15.9 (includes 15.1 - 15.8)	Release Notes Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Visual Studio 2019 version 16.0	Release Notes Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)	Release Notes Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1108						
Microsoft Visual Studio 2019 version 16.5	Release Notes Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
.NET Core 5.0	Release Notes Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for 32-bit Systems Service Pack 1	4556399 Monthly Rollup 4556403 Security Only	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for x64-based Systems Service Pack 1	4556399 Monthly Rollup 4556403 Security Only	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1108						
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for 32-bit systems	4556401 Monthly Rollup 4556405 Security Only	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for x64-based systems	4556401 Monthly Rollup 4556405 Security Only	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows RT 8.1	4556401 Monthly Rollup	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556399 Monthly Rollup 4556403 Security Only	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1108						
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4556399 Monthly Rollup 4556403 Security Only	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012	4556400 Monthly Rollup 4556404 Security Only	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 (Server Core installation)	4556400 Monthly Rollup 4556404 Security Only	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2	4556401 Monthly Rollup 4556405	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1108						
	Security Only					
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2 (Server Core installation)	4556401 Monthly Rollup 4556405 Security Only	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for 32-bit Systems	4552929 Security Update	Important	Denial of Service	4537479	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for x64-based Systems	4552929 Security Update	Important	Denial of Service	4537479	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server, version 1803 (Server Core Installation)	4552929 Security Update	Important	Denial of Service	4537479	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1108						
Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for 32-bit Systems	4552928 Security Update	Important	Denial of Service	4537478	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for x64-based Systems	4552928 Security Update	Important	Denial of Service	4537478	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for 32-bit Systems	4552926 Security Update	Important	Denial of Service	4537477	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for x64-based Systems	4552926 Security Update	Important	Denial of Service	4537477	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2016	4552926 Security	Important	Denial of Service	4537477	Base: N/A Temporal: N/A	Maybe

CVE-2020-1108						
	Update				Vector: N/A	
Microsoft .NET Framework 4.8 on Windows Server 2016 (Server Core installation)	4552926 Security Update	Important	Denial of Service	4537477	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 7 for 32-bit Systems Service Pack 1	4556399 Monthly Rollup 4556403 Security Only	Important	Denial of Service	4537477	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 7 for x64-based Systems Service Pack 1	4556399 Monthly Rollup 4556403 Security Only	Important	Denial of Service	4537477	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 8.1 for 32-bit systems	4556401 Monthly Rollup 4556405	Important	Denial of Service	4537477	Base: N/A Temporal: N/A	Maybe

CVE-2020-1108						
	Security Only				Vector: N/A	
Microsoft .NET Framework 4.8 on Windows 8.1 for x64-based systems	4556401 Monthly Rollup 4556405 Security Only	Important	Denial of Service	4537477	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows RT 8.1	4556401 Monthly Rollup	Important	Denial of Service	4537477	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556399 Monthly Rollup 4556403 Security Only	Important	Denial of Service	4537477	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4556399 Monthly Rollup 4556403	Important	Denial of Service	4537477	Base: N/A Temporal: N/A	Maybe

CVE-2020-1108						
	Security Only				Vector: N/A	
Microsoft .NET Framework 4.8 on Windows Server 2012	4556400 Monthly Rollup 4556404 Security Only	Important	Denial of Service	4537477	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 (Server Core installation)	4556400 Monthly Rollup 4556404 Security Only	Important	Denial of Service	4537477	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 R2	4556401 Monthly Rollup 4556405 Security Only	Important	Denial of Service	4537477	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 R2 (Server Core installation)	4556401 Monthly Rollup	Important	Denial of Service	4537477	Base: N/A Temporal: N/A	Maybe

CVE-2020-1108						
	4556405 Security Only				Vector: N/A	
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1809 for 32-bit Systems	4556441 Security Update	Important	Denial of Service	4538156	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1809 for x64-based Systems	4556441 Security Update	Important	Denial of Service	4538156	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server 2019	4556441 Security Update	Important	Denial of Service	4538156	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server 2019 (Server Core installation)	4556441 Security Update	Important	Denial of Service	4538156	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1108						
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1909 for 32-bit Systems	4552931 Security Update	Important	Denial of Service	4537572	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1909 for x64-based Systems	4552931 Security Update	Important	Denial of Service	4537572	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server, version 1909 (Server Core installation)	4552931 Security Update	Important	Denial of Service	4537572	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1903 for 32-bit Systems	4552931 Security Update	Important	Denial of Service	4537572	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1903 for x64-based Systems	4552931 Security	Important	Denial of Service	4537572	Base: N/A Temporal: N/A	Maybe

CVE-2020-1108						
	Update				Vector: N/A	
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server, version 1903 (Server Core installation)	4552931 Security Update	Important	Denial of Service	4537572	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Denial of Service	4550922	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Denial of Service	4550922	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Denial of Service	4550922	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2020-1108						
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1809 for 32-bit Systems	4556441 Security Update	Important	Denial of Service	4538156	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1809 for x64-based Systems	4556441 Security Update	Important	Denial of Service	4538156	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1809 for ARM64-based Systems	4556441 Security Update	Important	Denial of Service	4538156	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server 2019	4556441 Security Update	Important	Denial of Service	4538156	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server 2019 (Server Core installation)	4556441 Security	Important	Denial of Service	4538156	Base: N/A Temporal: N/A	Maybe

CVE-2020-1108						
	Update				Vector: N/A	
Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Denial of Service	4550929	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Denial of Service	4550929	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016	4556813 Security Update	Important	Denial of Service	4550929	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Denial of Service	4550929	Base: N/A Temporal: N/A Vector: N/A	Unknown

CVE-2020-1108						
Microsoft .NET Framework 3.5 AND 4.7.1/4.7.2 on Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Denial of Service	4550927	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 AND 4.7.1/4.7.2 on Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Denial of Service	4550927	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2	4556402 Monthly Rollup 4556406 Security Only	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6 on Windows Server 2008 for x64-based Systems Service Pack 2	4556402 Monthly Rollup 4556406 Security Only	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1108						
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4556402 Monthly Rollup 4556406 Security Only	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2	4556402 Monthly Rollup 4556406 Security Only	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2	4556402 Monthly Rollup 4556406 Security Only	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4556402 Monthly Rollup 4556406	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1108						
	Security Only					
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2	4556402 Monthly Rollup 4556406 Security Only	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2	4556402 Monthly Rollup 4556406 Security Only	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems	4556401 Monthly Rollup 4556405 Security Only	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems	4556401 Monthly Rollup	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A	Maybe

CVE-2020-1108						
	4556405 Security Only				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows Server 2012	4556400 Monthly Rollup 4556404 Security Only	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation)	4556400 Monthly Rollup 4556404 Security Only	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2	4556401 Monthly Rollup 4556405 Security Only	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation)	4556401 Monthly	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal:	Maybe

CVE-2020-1108						
	Rollup 4556405 Security Only				N/A Vector: N/A	
Microsoft .NET Framework 3.5.1 on Windows 7 for 32-bit Systems Service Pack 1	4556399 Monthly Rollup 4556403 Security Only	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows 7 for x64-based Systems Service Pack 1	4556399 Monthly Rollup 4556403 Security Only	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4556399 Monthly Rollup 4556403 Security Only	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1108						
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556399 Monthly Rollup 4556403 Security Only	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 7 for 32-bit Systems Service Pack 1	4556399 Monthly Rollup 4556403 Security Only	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 7 for x64-based Systems Service Pack 1	4556399 Monthly Rollup 4556403 Security Only	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems	4556401 Monthly Rollup 4556405	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1108						
	Security Only					
Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems	4556401 Monthly Rollup 4556405 Security Only	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows RT 8.1	4556401 Monthly Rollup	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4556402 Monthly Rollup 4556406 Security Only	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for x64-based Systems Service Pack 2	4556402 Monthly Rollup 4556406	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A	Maybe

CVE-2020-1108						
	Security Only				Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556399 Monthly Rollup 4556403 Security Only	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4556399 Monthly Rollup 4556403 Security Only	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012	4556400 Monthly Rollup 4556404 Security Only	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation)	4556400 Monthly Rollup	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A	Maybe

CVE-2020-1108						
	4556404 Security Only				Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2	4556401 Monthly Rollup 4556405 Security Only	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation)	4556401 Monthly Rollup 4556405 Security Only	Important	Denial of Service	4533098; 4535105	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1903 for ARM64-based Systems	4552931 Security Update	Important	Denial of Service	4537572	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1909 for ARM64-based Systems	4552931 Security	Important	Denial of Service	4537572	Base: N/A Temporal: N/A	Maybe

CVE-2020-1108						
	Update				Vector: N/A	
Microsoft .NET Framework 3.5 AND 4.7.1/4.7.2 on Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Denial of Service	4550927	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 AND 4.6/4.6.1/4.6.2 on Windows 10 for 32-bit Systems	4556826 Security Update	Important	Denial of Service	4550930	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 AND 4.6/4.6.1/4.6.2 on Windows 10 for x64-based Systems	4556826 Security Update	Important	Denial of Service	4550930	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Denial of Service	4550922	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2020-1109 - Windows Update Stack Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1109 MITRE NVD	**CVE Title:** Windows Update Stack Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows Update Stack fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application to take control of an affected system. The update addresses the vulnerability by correcting how the Windows Update Stack handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1109						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803	4556807 Security	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7	Yes

CVE-2020-1109						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1109						
based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1109						
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1109						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1110 - Windows Update Stack Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1110 MITRE NVD	**CVE Title:** Windows Update Stack Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows Update Stack fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application to take control of an affected system. The update addresses the vulnerability by correcting how the Windows Update Stack handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1110						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803	4556807 Security	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7	Yes

CVE-2020-1110						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1110						
based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1110						
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1110						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1111 - Windows Clipboard Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1111 MITRE NVD	**CVE Title:** Windows Clipboard Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Windows improperly handles calls to Clipboard Service. An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control over an affected system. The update addresses the vulnerability by correcting how Windows handles calls to Clipboard Service. **FAQ:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1111						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1809	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1111						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1111						
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1111						
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1112 - Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1112	**CVE Title:** Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability **Description:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	An elevation of privilege vulnerability exists when the Windows Background Intelligent Transfer Service (BITS) IIS module improperly handles uploaded content. An attacker who successfully exploited this vulnerability could upload restricted file types to an IIS-hosted folder. To exploit this vulnerability, an attacker would require permissions to upload files via BITS. An attacker could then submit a specially crafted request to upload a file. The security update addresses the vulnerability by correcting how Windows BITS validates file names. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1112						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-	4556807 Security	Important	Elevation of Privilege	4550922	Base: 8.5 Temporal: 7.6	Yes

CVE-2020-1112						
based Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1112						
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1112						
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1112						
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1112						
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for 32-bit Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1112						
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4556846 Monthly Rollup	Important	Elevation of Privilege	4550961	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems	4556860 Monthly Rollup 4556854 Security	Important	Elevation of Privilege	4550951	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1112						
Service Pack 2	Only					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security	Important	Elevation of Privilege	4550951	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1112						
	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems	4556836 Monthly Rollup 4556843 Security	Important	Elevation of Privilege	4550964	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1112						
Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2012	4556840 Monthly Rollup 4556852 Security Only	Important	Elevation of Privilege	4550917	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security	Important	Elevation of Privilege	4550917	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1112						
	Only					
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1113 - Windows Task Scheduler Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1113 MITRE NVD	**CVE Title:** Windows Task Scheduler Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists in Microsoft Windows when the Task Scheduler service fails to properly verify client connections over RPC. An attacker who successfully exploited this vulnerability could run arbitrary code as an administrator. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, a man-in-the-middle attacker would need to send a specially crafted request to a vulnerable system. The security update addresses the vulnerability by correcting how the Task Scheduler service validates connections. **FAQ:** None **Mitigations:**	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1113						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Security Feature Bypass	4550922	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1113						
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Security Feature Bypass	4550922	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Security Feature Bypass	4550922	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Security Feature Bypass	4550922	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Security Feature Bypass	4549949	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Security Feature Bypass	4549949	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1113						
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Security Feature Bypass	4549949	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Security Feature Bypass	4549949	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Security Feature Bypass	4549949	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Security Feature Bypass	4549951	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Security Feature Bypass	4549951	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909	4556799 Security	Important	Security Feature Bypass	4549951	Base: 5.3 Temporal: 4.8	Yes

CVE-2020-1113						
for ARM64-based Systems	Update				Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Security Feature Bypass	4549951	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Security Feature Bypass	4550927	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Security Feature Bypass	4550927	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Security Feature Bypass	4550927	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Security Feature Bypass	4549951	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1113						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Security Feature Bypass	4549951	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Security Feature Bypass	4549951	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Security Feature Bypass	4549951	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Security Feature Bypass	4550930	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Security Feature Bypass	4550930	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1113						
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Security Feature Bypass	4550929	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Security Feature Bypass	4550929	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Security Feature Bypass	4550929	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Security Feature Bypass	4550929	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows 7 for 32-bit Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Security Feature Bypass	4550964	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1113						
Windows 7 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Security Feature Bypass	4550964	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Security Feature Bypass	4550961	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Important	Security Feature Bypass	4550961	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1113						
Windows RT 8.1	4556846 Monthly Rollup	Important	Security Feature Bypass	4550961	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Security Feature Bypass	4550951	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Security Feature Bypass	4550951	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for Itanium-Based Systems	4556860 Monthly Rollup 4556854 Security	Important	Security Feature Bypass	4550951	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1113						
Service Pack 2	Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Security Feature Bypass	4550951	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Security Feature Bypass	4550951	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Security Feature Bypass	4550964	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1113						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Security Feature Bypass	4550964	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4556836 Monthly Rollup 4556843 Security Only	Important	Security Feature Bypass	4550964	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2012	4556840 Monthly Rollup 4556852 Security Only	Important	Security Feature Bypass	4550917	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1113						
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security Only	Important	Security Feature Bypass	4550917	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security Only	Important	Security Feature Bypass	4550961	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security Only	Important	Security Feature Bypass	4550961	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1114 - Windows Kernel Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1114 MITRE NVD	**CVE Title:** Windows Kernel Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application to take control of an affected system. The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1114						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803	4556807 Security	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7	Yes

CVE-2020-1114						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1114						
based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1114						
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1114						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1114						
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for 32-bit Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1114						
Windows 7 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1114						
Windows RT 8.1	4556846 Monthly Rollup	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for Itanium-Based	4556860 Monthly Rollup 4556854	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1114						
Systems Service Pack 2	Security Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for Itanium-Based	4556836 Monthly Rollup 4556843 Security	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1114						
Systems Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2012	4556840 Monthly Rollup 4556852	Important	Elevation of Privilege	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1114						
	Security Only					
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security Only	Important	Elevation of Privilege	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1114						
	Only					

CVE-2020-1116 - Windows CSRSS Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1116 MITRE NVD	**CVE Title:** Windows CSRSS Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows Client Server Run-Time Subsystem (CSRSS) fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application. The update addresses the vulnerability by correcting how the Windows CSRSS handles objects in memory. **FAQ:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	What type of information could be disclosed by this vulnerability? The type of information that could be disclosed if an attacker successfully exploited this vulnerability is the contents of Kernel memory. An attacker could read the contents of Kernel memory from a user mode process. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1116						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Information Disclosure	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Information Disclosure	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Information Disclosure	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Information Disclosure	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1116						
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1116						
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version	4556812 Security	Important	Information Disclosure	4550927	Base: 5.5 Temporal: 5	Yes

CVE-2020-1116						
1709 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Information Disclosure	4550927	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Information Disclosure	4550927	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1116						
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Information Disclosure	4550930	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Information Disclosure	4550930	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Information Disclosure	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1116						
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Information Disclosure	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Information Disclosure	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Information Disclosure	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 7 for 32-bit Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Information Disclosure	4550964	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 7 for x64-based	4556836 Monthly Rollup	Important	Information Disclosure	4550964	Base: 5.5 Temporal: 5	Unknown

CVE-2020-1116						
Systems Service Pack 1	4556843 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Information Disclosure	4550961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Important	Information Disclosure	4550961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4556846 Monthly Rollup	Important	Information Disclosure	4550961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1116						
Windows Server 2008 for 32-bit Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Information Disclosure	4550951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Information Disclosure	4550951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Information Disclosure	4550951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1116						
Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Information Disclosure	4550951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Information Disclosure	4550951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for Itanium-Based Systems	4556836 Monthly Rollup 4556843 Security Only	Important	Information Disclosure	4550964	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1116						
Service Pack 1						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Information Disclosure	4550964	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4556836 Monthly Rollup 4556843 Security Only	Important	Information Disclosure	4550964	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2012	4556840 Monthly Rollup 4556852 Security	Important	Information Disclosure	4550917	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1116						
	Only					
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security Only	Important	Information Disclosure	4550917	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security Only	Important	Information Disclosure	4550961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security Only	Important	Information Disclosure	4550961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1117 - Microsoft Color Management Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1117 MITRE NVD	**CVE Title:** Microsoft Color Management Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that the Color Management Module (ICM32.dll) handles objects in memory. An attacker who successfully exploited this vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability and then convince users to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to click a link in an email or Instant Messenger message that takes users to the attacker's website, or by opening an attachment sent through email.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how Color Management Module handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1117						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809	4551853 Security	Critical	Remote Code Execution	4549949	Base: 8.8 Temporal: 7.9	Unknown

CVE-2020-1117						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1117						
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1117						
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1117						
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1118 - Microsoft Windows Transport Layer Security Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1118 MITRE NVD	**CVE Title:** Microsoft Windows Transport Layer Security Denial of Service Vulnerability **Description:** A denial of service vulnerability exists in the Windows implementation of Transport Layer Security (TLS) when it improperly handles certain key exchanges. An attacker who successfully exploited the vulnerability could cause a target system to stop responding. To exploit this vulnerability, a remote unauthenticated attacker could send a specially crafted request to a target system utilizing TLS 1.2 or lower, triggering the system to automatically reboot. The update addresses the vulnerability by changing the way TLS key exchange messages are validated. **FAQ:** None **Mitigations:** None	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1118						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Denial of Service	4550922	Base: 8.6 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1118						
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Denial of Service	4550922	Base: 8.6 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Denial of Service	4550922	Base: 8.6 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Denial of Service	4550922	Base: 8.6 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Denial of Service	4549949	Base: 8.6 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Denial of Service	4549949	Base: 8.6 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1118						
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Denial of Service	4549949	Base: 8.6 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Denial of Service	4549949	Base: 8.6 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Denial of Service	4549949	Base: 8.6 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Denial of Service	4549951	Base: 8.6 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Denial of Service	4549951	Base: 8.6 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909	4556799 Security	Important	Denial of Service	4549951	Base: 8.6 Temporal: 7.7	Yes

CVE-2020-1118						
for ARM64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Denial of Service	4549951	Base: 8.6 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Denial of Service	4550927	Base: 8.6 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Denial of Service	4550927	Base: 8.6 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Denial of Service	4550927	Base: 8.6 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Denial of Service	4549951	Base: 8.6 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1118						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Denial of Service	4549951	Base: 8.6 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Denial of Service	4549951	Base: 8.6 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Denial of Service	4549951	Base: 8.6 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1121 - Windows Clipboard Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1121 MITRE NVD	**CVE Title:** Windows Clipboard Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Windows improperly handles calls to Clipboard Service. An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control over an affected system. The update addresses the vulnerability by correcting how Windows handles calls to Clipboard Service. **FAQ:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1121						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1809	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3	Unknown

CVE-2020-1121						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909	4556799 Security	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3	Yes

CVE-2020-1121						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1121						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1123 - Connected User Experiences and Telemetry Service Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1123 MITRE NVD	**CVE Title:** Connected User Experiences and Telemetry Service Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when Connected User Experiences and Telemetry Service improperly handles file operations. An attacker who successfully exploited this vulnerability could cause a system to stop responding. To exploit the vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability. The security update addresses the vulnerability by correcting how the Connected User Experiences and Telemetry Service handles file operations. **FAQ:** None **Mitigations:** None	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1123						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Denial of Service	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1123						
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Denial of Service	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Denial of Service	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Denial of Service	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Denial of Service	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Denial of Service	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1123						
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Denial of Service	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Denial of Service	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Denial of Service	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Denial of Service	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Denial of Service	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909	4556799 Security	Important	Denial of Service	4549951	Base: 5.5 Temporal: 5	Yes

CVE-2020-1123						
for ARM64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Denial of Service	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Denial of Service	4550927	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Denial of Service	4550927	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Denial of Service	4550927	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Denial of Service	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1123						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Denial of Service	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Denial of Service	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Denial of Service	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Denial of Service	4550930	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Denial of Service	4550930	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1123						
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Denial of Service	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Denial of Service	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Denial of Service	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Denial of Service	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1124 - Windows State Repository Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1124 MITRE NVD	**CVE Title:** Windows State Repository Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows State Repository Service handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1124						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803	4556807 Security	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7	Yes

CVE-2020-1124						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1124						
based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1124						
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1124						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1124						
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1125 - Windows Runtime Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1125 MITRE NVD	**CVE Title:** Windows Runtime Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows Runtime handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1125						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1125						
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1125						
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1125						
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1125						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1125						
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1125						
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4556846 Monthly Rollup	Important	Elevation of Privilege	4550961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1126 - Media Foundation Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1126	**CVE Title:** Media Foundation Memory Corruption Vulnerability **Description:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory. An attacker who successfully exploited the vulnerability could install programs; view, change, or delete data; or create new accounts with full user rights. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit a malicious webpage. The security update addresses the vulnerability by correcting how Windows Media Foundation handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1126						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-	4556807 Security	Critical	Remote Code Execution	4550922	Base: 8.8 Temporal: 7.9	Yes

CVE-2020-1126						
based Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1126						
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1126						
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1126						
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1131 - Windows State Repository Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1131 MITRE NVD	**CVE Title:** Windows State Repository Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows State Repository Service handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1131						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803	4556807 Security	Important	Elevation of Privilege	4550922	Base: 5.5 Temporal: 5	Yes

CVE-2020-1131						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-	4551853 Security	Important	Elevation of Privilege	4549949	Base: 5.5 Temporal: 5	Unknown

CVE-2020-1131						
based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1131						
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1131						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1131						
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1132 - Windows Error Reporting Manager Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1132 MITRE NVD	**CVE Title:** Windows Error Reporting Manager Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles file and folder links. An attacker who successfully exploited this vulnerability could overwrite a targeted file leading to an elevated status. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The security update addresses the vulnerability by correcting how Windows Error Reporting manager handles file and folder links. **FAQ:** None **Mitigations:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1132						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1132						
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1132						
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1132						
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1132						
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1132						
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1134 - Windows State Repository Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1134 MITRE NVD	**CVE Title:** Windows State Repository Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows State Repository Service handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1134						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803	4556807 Security	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7	Yes

CVE-2020-1134						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1134						
based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1134						
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1134						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1134						
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1135 - Windows Graphics Component Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1135 MITRE NVD	**CVE Title:** Windows Graphics Component Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run processes in an elevated context. In a local attack scenario, an attacker could exploit this vulnerability by running a specially crafted application to take control over the affected system. The update addresses the vulnerability by correcting the way in which the Microsoft Graphics Component handles objects in memory and preventing unintended elevation from user mode. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1135						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803	4556807 Security	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7	Yes

CVE-2020-1135						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1135						
based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1135						
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1135						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1136 - Media Foundation Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1136 MITRE NVD	**CVE Title:** Media Foundation Memory Corruption Vulnerability **Description:** A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory. An attacker who successfully exploited the vulnerability could install programs; view, change, or delete data; or create new accounts with full user rights. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit a malicious webpage. The security update addresses the vulnerability by correcting how Windows Media Foundation handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1136						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803	4556807 Security	Critical	Remote Code Execution	4550922	Base: 7.8 Temporal: 7	Yes

CVE-2020-1136						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-	4551853 Security	Critical	Remote Code Execution	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1136						
based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2019	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1136						
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1136						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Critical	Remote Code Execution	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Critical	Remote Code Execution	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1136						
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Critical	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1136						
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Critical	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4556846 Monthly Rollup	Critical	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security Only	Critical	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security	Critical	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1136						
	Only					

CVE-2020-1137 - Windows Push Notification Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1137 MITRE NVD	**CVE Title:** Windows Push Notification Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way the Windows Push Notification Service handles objects in memory. An attacker who successfully exploited this vulnerability could run processes in an elevated context. An attacker could then install programs; view, change or delete data. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how the Windows Push Notification Service handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1137						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1137						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1137						
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1137						
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1138 - Windows Storage Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1138 MITRE NVD	**CVE Title:** Windows Storage Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations. An attacker who successfully exploited this vulnerability could gain elevated privileges on the victim system. To exploit the vulnerability, an attacker would first have to gain execution on the victim system, then run a specially crafted application. The security update addresses the vulnerability by correcting how the Storage Services handles file operations. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1138						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909	4556799 Security	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3	Yes

CVE-2020-1138						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3	Unknown

CVE-2020-1138						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1138						
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1138						
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1138						
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1139 - Windows Runtime Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1139 MITRE NVD	**CVE Title:** Windows Runtime Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows Runtime handles objects in memory. **FAQ:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1139						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803	4556807 Security	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7	Yes

CVE-2020-1139						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1139						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1139						
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1139						
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1139						
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1140 - DirectX Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1140 MITRE NVD	**CVE Title:** DirectX Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses the vulnerability by correcting how DirectX handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1140						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1140						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1140						
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1140						
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1141 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1141 MITRE NVD	**CVE Title:** Windows GDI Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system. By itself, the information disclosure does not allow arbitrary code execution; however, it could allow arbitrary code to be run if the attacker uses it in combination with another vulnerability. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how GDI handles memory addresses. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is memory layout - the vulnerability allows an attacker to collect information that facilitates predicting addressing of the memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1141						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Information Disclosure	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Information Disclosure	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Information Disclosure	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1141						
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Information Disclosure	4550922	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5	Unknown

CVE-2020-1141						
	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Information Disclosure	4549949	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server,	4556799 Security	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5	Yes

CVE-2020-1141						
version 1909 (Server Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Information Disclosure	4550927	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Information Disclosure	4550927	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Information Disclosure	4550927	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1141						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Information Disclosure	4550930	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-	4556826 Security	Important	Information Disclosure	4550930	Base: 5.5 Temporal: 5	Yes

CVE-2020-1141						
based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Information Disclosure	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Information Disclosure	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Information Disclosure	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Information Disclosure	4550929	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 7 for 32-bit Systems	4556836 Monthly Rollup 4556843	Important	Information Disclosure	4550964	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1141						
Service Pack 1	Security Only					
Windows 7 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Information Disclosure	4550964	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Information Disclosure	4550961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security	Important	Information Disclosure	4550961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1141						
	Only					
Windows RT 8.1	4556846 Monthly Rollup	Important	Information Disclosure	4550961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Information Disclosure	4550951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Information Disclosure	4550951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008	4556860 Monthly	Important	Information Disclosure	4550951	Base: 5.5 Temporal: 5	Unknown

CVE-2020-1141						
for Itanium-Based Systems Service Pack 2	Rollup 4556854 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Information Disclosure	4550951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Information Disclosure	4550951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008	4556836 Monthly	Important	Information Disclosure	4550964	Base: 5.5 Temporal: 5	Unknown

CVE-2020-1141						
R2 for Itanium-Based Systems Service Pack 1	Rollup 4556843 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Information Disclosure	4550964	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4556836 Monthly Rollup 4556843 Security Only	Important	Information Disclosure	4550964	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-1141						
Windows Server 2012	4556840 Monthly Rollup 4556852 Security Only	Important	Information Disclosure	4550917	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security Only	Important	Information Disclosure	4550917	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security Only	Important	Information Disclosure	4550961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4556846 Monthly	Important	Information Disclosure	4550961	Base: 5.5 Temporal: 5	Yes

CVE-2020-1141						
R2 (Server Core installation)	Rollup 4556853 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	

CVE-2020-1142 - Windows GDI Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1142 MITRE NVD	**CVE Title:** Windows GDI Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The update addresses the vulnerability by correcting how GDI handles objects in memory and by preventing instances of unintended user-mode privilege elevation. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1142						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1142						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1142						
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1142						
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1143 - Win32k Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1143 MITRE NVD	**CVE Title:** Win32k Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how the Windows kernel-mode driver handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1143						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1143						
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1143						
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1143						
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1143						
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1143						
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for 32-bit Systems	4556836 Monthly Rollup	Important	Elevation of Privilege	4550964	Base: 7 Temporal: 6.3	Unknown

CVE-2020-1143						
Service Pack 1	4556843 Security Only				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 7 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security	Important	Elevation of Privilege	4550961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1143						
	Only					
Windows RT 8.1	4556846 Monthly Rollup	Important	Elevation of Privilege	4550961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1143						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1143						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1143						
Core installation)						
Windows Server 2012	4556840 Monthly Rollup 4556852 Security Only	Important	Elevation of Privilege	4550917	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security Only	Important	Elevation of Privilege	4550917	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1143						
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1144 - Windows State Repository Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1144 MITRE NVD	**CVE Title:** Windows State Repository Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows State Repository Service handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1144						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1144						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1144						
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1144						
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1144						
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1144						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	

CVE-2020-1145 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1145 MITRE NVD	**CVE Title:** Windows GDI Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system. By itself, the information disclosure does not allow arbitrary code execution; however, it could allow arbitrary code to be run if the attacker uses it in combination with another vulnerability. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how GDI handles memory addresses.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1145						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1145						
Core installation)						
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server	4556799 Security Update	Important	Information Disclosure	4549951	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-1145						
Core installation)						

CVE-2020-1149 - Windows Runtime Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1149 MITRE NVD	**CVE Title:** Windows Runtime Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows Runtime handles objects in memory. **FAQ:** None **Mitigations:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1149						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1149						
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1149						
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1149						
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1149						
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1149						
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup	Important	Elevation of Privilege	4550961	Base: 7 Temporal: 6.3	Yes

CVE-2020-1149						
	4556853 Security Only				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4556846 Monthly Rollup	Important	Elevation of Privilege	4550961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1149						
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1150 - Media Foundation Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1150 MITRE NVD	**CVE Title:** Media Foundation Memory Corruption Vulnerability **Description:** A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory. An attacker who successfully exploited the vulnerability could install programs; view, change, or delete data; or create new accounts with full user rights. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit a malicious webpage.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how Windows Media Foundation handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1150						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for Itanium-Based Systems	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1150						
Service Pack 1						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1151 - Windows Runtime Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1151 MITRE NVD	**CVE Title:** Windows Runtime Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows Runtime handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1151						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1151						
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1151						
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1151						
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1151						
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1153 - Microsoft Graphics Components Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1153 MITRE NVD	**CVE Title:** Microsoft Graphics Components Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary code on a target system. To exploit the vulnerability, a user would have to open a specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Graphics Components handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1153						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1153						
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Critical	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1153						
Windows Server 2019	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Critical	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909	4556799 Security	Critical	Remote Code Execution	4549951	Base: 7.8 Temporal: 7	Yes

CVE-2020-1153						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Critical	Remote Code Execution	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1153						
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Critical	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Critical	Remote Code Execution	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Critical	Remote Code Execution	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1153						
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Critical	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for 32-bit Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Critical	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for x64-based Systems	4556836 Monthly Rollup 4556843	Critical	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1153						
Service Pack 1	Security Only					
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Critical	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Critical	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4556846 Monthly Rollup	Critical	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1153						
Windows Server 2008 for 32-bit Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Critical	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Critical	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Critical	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1153						
Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Critical	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Critical	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Critical	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1153						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Critical	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4556836 Monthly Rollup 4556843 Security Only	Critical	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2012	4556840 Monthly Rollup 4556852 Security Only	Critical	Remote Code Execution	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1153						
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security Only	Critical	Remote Code Execution	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security Only	Critical	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security Only	Critical	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1154 - Windows Common Log File System Driver Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1154 MITRE NVD	**CVE Title:** Windows Common Log File System Driver Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run processes in an elevated context. To exploit the vulnerability, an attacker would first have to log on to the system, and then run a specially crafted application to take control over the affected system. The security update addresses the vulnerability by correcting how CLFS handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1154						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803	4556807 Security	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7	Yes

CVE-2020-1154						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1154						
based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1154						
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1154						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1154						
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for 32-bit Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1154						
Windows 7 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1154						
Windows RT 8.1	4556846 Monthly Rollup	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for Itanium-Based	4556860 Monthly Rollup 4556854	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1154						
Systems Service Pack 2	Security Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4556860 Monthly Rollup 4556854 Security Only	Important	Elevation of Privilege	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for Itanium-Based	4556836 Monthly Rollup 4556843 Security	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1154						
Systems Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4556836 Monthly Rollup 4556843 Security Only	Important	Elevation of Privilege	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2012	4556840 Monthly Rollup 4556852	Important	Elevation of Privilege	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1154						
	Security Only					
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security Only	Important	Elevation of Privilege	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security Only	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security	Important	Elevation of Privilege	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1154						
	Only					

CVE-2020-1155 - Windows Runtime Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1155 MITRE NVD	**CVE Title:** Windows Runtime Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows Runtime handles objects in memory. **FAQ:** None **Mitigations:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1155						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1155						
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1155						
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1155						
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1155						
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1156 - Windows Runtime Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1156 MITRE NVD	**CVE Title:** Windows Runtime Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows Runtime handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1156						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1156						
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1156						
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1156						
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1156						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1156						
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1157 - Windows Runtime Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1157 MITRE NVD	**CVE Title:** Windows Runtime Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows Runtime handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1157						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1157						
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1157						
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1157						
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1157						
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1157						
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1158 - Windows Runtime Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1158 MITRE NVD	**CVE Title:** Windows Runtime Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows Runtime handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1158						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1158						
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1158						
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1158						
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1158						
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1158						
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1161 - ASP.NET Core Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1161 MITRE NVD	**CVE Title:** ASP.NET Core Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when ASP.NET Core improperly handles web requests. An attacker who successfully exploited this vulnerability could cause a denial of service against an ASP.NET Core web application. The vulnerability can be exploited remotely, without authentication.	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	A remote unauthenticated attacker could exploit this vulnerability by issuing specially crafted requests to the ASP.NET Core application. The update addresses the vulnerability by correcting how the ASP.NET Core web application handles web requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1161						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Visual Studio 2017 version 15.9 (includes 15.1 - 15.8)	Release Notes Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Visual Studio 2019 version 16.0	Release Notes Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)	Release Notes Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Visual Studio 2019 version 16.5	Release Notes Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
ASP.NET Core 3.1	Release Notes Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1164 - Windows Runtime Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1164 MITRE NVD	**CVE Title:** Windows Runtime Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows Runtime handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1164						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1164						
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1164						
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1164						
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1164						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Elevation of Privilege	4550930	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1164						
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1165 - Windows Clipboard Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1165 MITRE NVD	**CVE Title:** Windows Clipboard Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Windows improperly handles calls to Clipboard Service. An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control over an affected system. The update addresses the vulnerability by correcting how Windows handles calls to Clipboard Service. **FAQ:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1165						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1909	4556799 Security	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7	Yes

CVE-2020-1165						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903	4556799 Security	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7	Yes

CVE-2020-1165						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1166 - Windows Clipboard Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1166 MITRE NVD	**CVE Title:** Windows Clipboard Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Windows improperly handles calls to Clipboard Service. An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control over an affected system. The update addresses the vulnerability by correcting how Windows handles calls to Clipboard Service. **FAQ:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1166						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1909	4556799 Security	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7	Yes

CVE-2020-1166						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903	4556799 Security	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7	Yes

CVE-2020-1166						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1171 - Visual Studio Code Python Extension Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1171 MITRE NVD	**CVE Title:** Visual Studio Code Python Extension Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Visual Studio Code when the Python extension loads configuration files after opening a project. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would need to convince a target to clone a repository and open it in Visual Studio Code with the Python extension installed. Attacker-specified code would execute when the target opened the integrated terminal. The update address the vulnerability by modifying the way Visual Studio Code Python extension handles environment variables.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1171						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2020-1171						
Visual Studio Code	Release Notes Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1173 - Microsoft Power BI Report Server Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1173 MITRE NVD	**CVE Title:** Microsoft Power BI Report Server Spoofing Vulnerability **Description:** A spoofing vulnerability exists in Microsoft Power BI Report Server in the way it validates the content-type of uploaded attachments. An authenticated attacker could exploit the vulnerability by uploading a specially crafted payload and sending it to the user. The attacker who successfully exploited this vulnerability could then perform actions and run scripts in the security context of the user. This security update addresses the vulnerability by ensuring Power BI Report Server properly validates content-type of the attachments when uploading and opening. **FAQ:**	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	What version of Power BI has this vulnerability? • The version of Power BI that contains the vulnerability is the May 2019 Release, version 1.5.7074.36177 (Build 15.0.1102.371). • The vulnerability was addressed in the September 2019 release, version 1.6.7236.4246 (Build 15.0.1102.646). • The most recent version of Power BI is the January 2020 release build is 15.0.1102.777. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1173						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Power BI Report Server	Release Details Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-1174 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1174 MITRE NVD	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1174						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809	4551853 Security	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1174						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1174						
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1174						
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1174						
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Remote Code Execution	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Remote Code Execution	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security	Important	Remote Code Execution	4550929	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1174						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 7 for 32-bit Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1174						
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4556846 Monthly Rollup	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack	4556860 Monthly Rollup 4556854 Security	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1174						
2 (Server Core installation)	Only					
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server	4556860 Monthly Rollup 4556854 Security	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1174						
Core installation)	Only					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack	4556836 Monthly Rollup 4556843 Security	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1174						
1 (Server Core installation)	Only					
Windows Server 2012	4556840 Monthly Rollup 4556852 Security Only	Important	Remote Code Execution	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security Only	Important	Remote Code Execution	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1174						
	Only					
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security Only	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1175 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1175 MITRE NVD	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1175						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809	4551853 Security	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1175						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1175						
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1175						
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1175						
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Remote Code Execution	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Remote Code Execution	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security	Important	Remote Code Execution	4550929	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1175						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 7 for 32-bit Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1175						
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4556846 Monthly Rollup	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack	4556860 Monthly Rollup 4556854 Security	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1175						
2 (Server Core installation)	Only					
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server	4556860 Monthly Rollup 4556854 Security	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1175						
Core installation)	Only					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack	4556836 Monthly Rollup 4556843 Security	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1175						
1 (Server Core installation)	Only					
Windows Server 2012	4556840 Monthly Rollup 4556852 Security Only	Important	Remote Code Execution	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security Only	Important	Remote Code Execution	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1175						
	Only					
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security Only	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1176 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1176 MITRE NVD	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1176						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Remote Code Execution	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809	4551853 Security	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1176						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Remote Code Execution	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1176						
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1176						
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Remote Code Execution	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Remote Code Execution	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1176						
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Remote Code Execution	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4556826 Security Update	Important	Remote Code Execution	4550930	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Remote Code Execution	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security	Important	Remote Code Execution	4550929	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1176						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 7 for 32-bit Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 7 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1176						
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4556846 Monthly Rollup	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack	4556860 Monthly Rollup 4556854 Security	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1176						
2 (Server Core installation)	Only					
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2	4556860 Monthly Rollup 4556854 Security Only	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server	4556860 Monthly Rollup 4556854 Security	Important	Remote Code Execution	4550951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1176						
Core installation)	Only					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack	4556836 Monthly Rollup 4556843 Security	Important	Remote Code Execution	4550964	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1176						
1 (Server Core installation)	Only					
Windows Server 2012	4556840 Monthly Rollup 4556852 Security Only	Important	Remote Code Execution	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security Only	Important	Remote Code Execution	4550917	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1176						
	Only					
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security Only	Important	Remote Code Execution	4550961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1179 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1179 MITRE NVD	**CVE Title:** Windows GDI Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how the Windows GDI component handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is memory layout - the vulnerability allows an attacker to collect information that facilitates predicting addressing of the memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1179						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Information Disclosure	4550922	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Information Disclosure	4550922	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Information Disclosure	4550922	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Information Disclosure	4550922	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2020-1179						
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Information Disclosure	4549949	Base: N/A Temporal: N/A Vector: N/A	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Information Disclosure	4549949	Base: N/A Temporal: N/A Vector: N/A	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Information Disclosure	4549949	Base: N/A Temporal: N/A Vector: N/A	Unknown
Windows Server 2019	4551853 Security Update	Important	Information Disclosure	4549949	Base: N/A Temporal: N/A Vector: N/A	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Information Disclosure	4549949	Base: N/A Temporal: N/A Vector: N/A	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: N/A Temporal:	Yes

CVE-2020-1179						
					N/A Vector: N/A	
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Information Disclosure	4549951	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Information Disclosure	4550927	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Information Disclosure	4550927	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2020-1179						
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Information Disclosure	4550927	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Information Disclosure	4549951	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Information Disclosure	4549951	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 for 32-bit Systems	4556826 Security Update	Important	Information Disclosure	4550930	Base: N/A Temporal:	Yes

CVE-2020-1179						
					N/A Vector: N/A	
Windows 10 for x64-based Systems	4556826 Security Update	Important	Information Disclosure	4550930	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Information Disclosure	4550929	Base: N/A Temporal: N/A Vector: N/A	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Information Disclosure	4550929	Base: N/A Temporal: N/A Vector: N/A	Unknown
Windows Server 2016	4556813 Security Update	Important	Information Disclosure	4550929	Base: N/A Temporal: N/A Vector: N/A	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Information Disclosure	4550929	Base: N/A Temporal: N/A Vector: N/A	Unknown

CVE-2020-1179						
Windows 7 for 32-bit Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Information Disclosure	4550964	Base: N/A Temporal: N/A Vector: N/A	Unknown
Windows 7 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Information Disclosure	4550964	Base: N/A Temporal: N/A Vector: N/A	Unknown
Windows 8.1 for 32-bit systems	4556846 Monthly Rollup 4556853 Security Only	Important	Information Disclosure	4550961	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 8.1 for x64-based systems	4556846 Monthly Rollup 4556853 Security Only	Important	Information Disclosure	4550961	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows RT 8.1	4556846 Monthly Rollup	Important	Information Disclosure	4550961	Base: N/A Temporal:	Yes

CVE-2020-1179						
					N/A Vector: N/A	
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Information Disclosure	4550964	Base: N/A Temporal: N/A Vector: N/A	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4556836 Monthly Rollup 4556843 Security Only	Important	Information Disclosure	4550964	Base: N/A Temporal: N/A Vector: N/A	Unknown
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4556836 Monthly Rollup 4556843 Security Only	Important	Information Disclosure	4550964	Base: N/A Temporal: N/A Vector: N/A	Unknown
Windows Server 2012	4556840 Monthly Rollup 4556852 Security Only	Important	Information Disclosure	4550917	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2020-1179						
Windows Server 2012 (Server Core installation)	4556840 Monthly Rollup 4556852 Security Only	Important	Information Disclosure	4550917	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 R2	4556846 Monthly Rollup 4556853 Security Only	Important	Information Disclosure	4550961	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 R2 (Server Core installation)	4556846 Monthly Rollup 4556853 Security Only	Important	Information Disclosure	4550961	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2020-1184 - Windows State Repository Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1184 MITRE NVD	**CVE Title:** Windows State Repository Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows State Repository Service handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1184						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803	4556807 Security	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7	Yes

CVE-2020-1184						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1184						
based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1184						
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1184						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1184						
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1185 - Windows State Repository Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1185 MITRE NVD	**CVE Title:** Windows State Repository Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows State Repository Service handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1185						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1185						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1185						
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1185						
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1185						
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1186 - Windows State Repository Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1186 MITRE NVD	**CVE Title:** Windows State Repository Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows State Repository Service handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1186						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803	4556807 Security	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7	Yes

CVE-2020-1186						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1186						
based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1186						
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1186						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1186						
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1187 - Windows State Repository Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1187 MITRE NVD	**CVE Title:** Windows State Repository Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows State Repository Service handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1187						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1187						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1187						
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1187						
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1187						
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1188 - Windows State Repository Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1188 MITRE NVD	**CVE Title:** Windows State Repository Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows State Repository Service handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1188						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803	4556807 Security	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7	Yes

CVE-2020-1188						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1188						
based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1188						
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1188						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1188						
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1189 - Windows State Repository Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1189 MITRE NVD	**CVE Title:** Windows State Repository Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows State Repository Service handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1189						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1189						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1189						
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1189						
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1189						
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1190 - Windows State Repository Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1190 MITRE NVD	**CVE Title:** Windows State Repository Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows State Repository Service handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1190						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803	4556807 Security	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7	Yes

CVE-2020-1190						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1190						
based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1190						
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1190						
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1190						
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-1191 - Windows State Repository Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1191 MITRE NVD	**CVE Title:** Windows State Repository Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in an elevated context.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	An attacker could exploit this vulnerability by running a specially crafted application on the victim system. The update addresses the vulnerability by correcting the way the Windows State Repository Service handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1191						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4556807 Security Update	Important	Elevation of Privilege	4550922	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809	4551853 Security	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7	Unknown

CVE-2020-1191						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-based Systems	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4551853 Security Update	Important	Elevation of Privilege	4549949	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1191						
Windows 10 Version 1909 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1191						
Windows 10 Version 1709 for ARM64-based Systems	4556812 Security Update	Important	Elevation of Privilege	4550927	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4556799 Security Update	Important	Elevation of Privilege	4549951	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-1191						
Windows 10 Version 1607 for 32-bit Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4556813 Security Update	Important	Elevation of Privilege	4550929	Base: N/A Temporal: N/A Vector: N/A	Unknown

CVE-2020-1192 - Visual Studio Code Python Extension Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-1192 MITRE NVD	**CVE Title:** Visual Studio Code Python Extension Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Visual Studio Code when the Python extension loads workspace settings from a notebook file. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would need to convince a target to open a specially crafted file in Visual Studio Code with the Python extension installed. The update address the vulnerability by modifying the way Visual Studio Code Python extension enforces user settings. **FAQ:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/12/2020 07:00:00 Information published.		

Affected Software

The following tables list the affected software details for the vulnerability.

CVE-2020-1192						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Visual Studio Code	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe

Statement

This advisory is only used to describe a potential risk. NSFOCUS does not provide any commitment or promise on this advisory. NSFOCUS and the author will not bear any liability for any direct and/or indirect consequences and losses caused by transmitting and/or using this advisory. NSFOCUS reserves all the rights to modify and interpret this advisory. Please include this statement paragraph when reproducing or transferring this advisory. Do not modify this advisory, add/delete any information to/from it, or use this advisory for commercial purposes without permission from NSFOCUS.

About NSFOCUS

NSFOCUS, Inc., a global network and cyber security leader, protects enterprises and carriers from advanced cyber attacks. The company's Intelligent Hybrid Security strategy utilizes both cloud and on-premises security platforms, built on a foundation of real-time global threat intelligence, to provide multi-layered, unified and dynamic protection against advanced cyber attacks.

NSFOCUS works with Fortune Global 500 companies, including four of the world's five largest financial institutions, organizations in insurance, retail, healthcare, critical infrastructure industries as well as government agencies. NSFOCUS has technology and channel partners in more than 60 countries, is a member of both the Microsoft Active Protections Program (MAPP), and the Cloud Security Alliance (CSA).

A wholly owned subsidiary of NSFOCUS Technologies Group Co., Ltd., the company has operations in the Americas, Europe, the Middle East and Asia Pacific.