Microsoft Security Update for January 2020 Fixes 49 Security Vulnerabilities

Overview

Microsoft released the January security update on Tuesday, fixing 49 security issues ranging from simple spoofing attacks to remote code execution, discovered in products like .NET Framework, Apps, ASP.NET, Common Log File System Driver, Microsoft Dynamics, Microsoft Graphics Component, Microsoft Office, Microsoft Scripting Engine, Microsoft Windows, Microsoft Windows Search Component, Windows Hyper-V, Windows Media, Windows RDP, Windows Subsystem for Linux, and Windows Update Stack.

Of the vulnerabilities fixed by Microsoft's this monthly update, a total of eight critical vulnerabilities exist in the .NET Framework, ASP.NET, Microsoft Scripting Engine, and Windows RDP. In addition, there are 41 important vulnerabilities.

Critical Vulnerabilities

The following are eight critical vulnerabilities covered in this update.

Windows RDP

- **CVE-2020-0609、CVE-2020-0610**

  These two remote code execution vulnerabilities in the Windows Remote Desktop Gateway (RD Gateway) could be exploited by unauthenticated attackers.

If the two vulnerabilities are exploited successfully, arbitrary code may be executed on the target system, allowing the attacker to install the program, view, change or delete data, or create a new account with full user rights.
To exploit this vulnerability, an attacker needs to send a specially crafted request to the RD gateway of the target system via RDP.
This update addresses these issues by correcting the way the RD gateway handles connection requests.
For more details about the vulnerabilities and download updates, please refer to Microsoft's official security advisories:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0609
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0610

- **CVE-2020-0611**

This is a remote code execution vulnerability in Windows Remote Desktop clients.
An attacker who successfully exploited this vulnerability could execute arbitrary code on a user's computer connected to a malicious server. After that, an attacker could install a malicious program, view, change, or delete data, or create a new account with full user rights.
To exploit this vulnerability, an attacker needs to take control of the server and then convinces a user to connect to the server. This vulnerability could be triggered if a user accesses a malicious server. Although attackers cannot force users to connect to malicious servers, they may entice users to connect through social engineering, DNS poisoning, or man-in-the-middle (MITM) technology. An attacker could also compromise a legitimate server, host malicious code on it, and wait for users to connect.

For more details about the vulnerabilities and download updates, please refer to Microsoft's official security advisories:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0611

Microsoft Scripting Engine

- **CVE-2020-0640**

This is a memory corruption vulnerability in the way Internet Explorer handles objects in memory. The vulnerability allows an attacker to execute arbitrary code in the context of the current user.
An attacker who successfully exploited this vulnerability could gain the same user rights as the current user. If the current user logs in with administrative privileges, an attacker could take control of the affected system and may then install a malicious program, view, change or delete data, or create a new account with full user privileges.
An attacker could build a specially crafted website and then convince users to visit the website. However, attackers cannot force users to view malicious contents, but entice users by email or instant messaging instead.
Internet Explorer 9, 10, and 11 are affected.
For more details about the vulnerabilities and download updates, please refer to Microsoft's official security advisories:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0640

ASP.NET and .NET Framework

- **CVE-2020-0603, CVE-2020-0605, CVE-2020-0606, and CVE-2020-0646**

The above vulnerabilities are remote code execution vulnerabilities in .NET and ASP.NET Core software. These vulnerabilities can be triggered if a user opens a maliciously crafted file while using an affected .NET or ASP.NET Core version. With a successful exploitation, an attacker could execute arbitrary code in the context of the current user. These errors exist in the way the software handles memory objects.

For more details about the vulnerabilities and download updates, please refer to Microsoft's official security advisories:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0603
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0605
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0606
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0646

Important Vulnerabilities

In addition to critical vulnerabilities, this update also fixes 41 important vulnerabilities, three of which require more attention as follows.

CVE-2020-0601

This is a spoofing vulnerability in Windows CryptoAPI. As the Elliptic Curve Cryptography certificate was incorrectly verified by crypt32.dll, an attacker could use this error to spoof a code signing certificate and secretly sign a file, making the file appear to come from a trusted source. Attackers could also use this vulnerability to conduct man-in-the-middle attacks and decrypt confidential information.
For more details about the vulnerabilities and download updates, please refer to Microsoft's official security advisories:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601

CVE-2020-0616

This is a Microsoft Windows denial-of-service vulnerability. The vulnerability exists when Windows cannot properly handle hard links. An attacker who successfully exploits this vulnerability could cause the target system to stop responding.
An attacker must log in to the victim's computer to exploit this vulnerability and then run a specially designed application that could allow the attacker to overwrite system files.
For more details about the vulnerabilities and download updates, please refer to Microsoft's official security advisories:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0616

CVE-2020-0654

A security feature bypass vulnerability exists in Android's Microsoft OneDrive application. This could allow an attacker to bypass the password or fingerprint of the application.
For more details about the vulnerabilities and download updates, please refer to Microsoft's official security advisories:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0654

Remediation

Bugs fixed in this update are shown in the following table:

Product	CVE ID	CVE Title	Severity Level

.NET Framework	CVE-2020-0605	.NET Framework Remote code execution vulnerability	Critical
.NET Framework	CVE-2020-0606	.NET Framework Remote code execution vulnerability	Critical
.NET Framework	CVE-2020-0646	.NET Framework Remote Code Execution Injection Vulnerability	Critical
Apps	CVE-2020-0654	Microsoft OneDrive for Android Security feature bypass vulnerability	Important
ASP.NET	CVE-2020-0602	ASP.NET Core Denial of service vulnerability	Important
ASP.NET	CVE-2020-0603	ASP.NET Core Remote code execution vulnerability	Critical
Common Log File System Driver	CVE-2020-0615	Windows Common Log File System Driver Information Disclosure Vulnerability	Important

Common Log File System Driver	CVE-2020-0639	Windows Common Log File System Driver Information Disclosure Vulnerability	Important
Common Log File System Driver	CVE-2020-0634	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Important
Microsoft Dynamics	CVE-2020-0656	Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability	Important
Microsoft Graphics Component	CVE-2020-0607	Microsoft Graphics Components Information Disclosure Vulnerability	Important
Microsoft Graphics Component	CVE-2020-0622	Microsoft Graphics Component Information Disclosure Vulnerability	Important
Microsoft Graphics Component	CVE-2020-0642	Win32k Elevation of Privilege Vulnerability	Important

Microsoft Graphics Component	CVE-2020-0643	Windows GDI+ Information Disclosure Vulnerability	Important
Microsoft Office	CVE-2020-0647	Microsoft Office Online Fraud	Important
Microsoft Office	CVE-2020-0650	Microsoft Excel Remote code execution vulnerability	Important
Microsoft Office	CVE-2020-0651	Microsoft Excel Remote code execution vulnerability	Important
Microsoft Office	CVE-2020-0652	Microsoft Office Memory corruption	Important
Microsoft Office	CVE-2020-0653	Microsoft Excel Remote code execution vulnerability	Important
Microsoft Scripting Engine	CVE-2020-0640	Internet Explorer Memory corruption	Critical
Microsoft Windows	CVE-2020-0601	Windows CryptoAPI Fraud	Important

Microsoft Windows	CVE-2020-0608	Win32k Information Disclosure Vulnerability	Important
Microsoft Windows	CVE-2020-0616	Microsoft Windows Denial of service vulnerability	Important
Microsoft Windows	CVE-2020-0620	Microsoft Cryptographic Services Elevation of Privilege Vulnerability	Important
Microsoft Windows	CVE-2020-0621	Windows Security feature bypass vulnerability	Important
Microsoft Windows	CVE-2020-0624	Win32k Elevation of Privilege Vulnerability	Important
Microsoft Windows	CVE-2020-0635	Windows Elevation of Privilege Vulnerability	Important
Microsoft Windows	CVE-2020-0644	Windows Elevation of Privilege Vulnerability	Important

Microsoft Windows Search Component	CVE-2020-0613	Windows Search Indexer Elevation of Privilege Vulnerability	Important
Microsoft Windows Search Component	CVE-2020-0614	Windows Search Indexer Elevation of Privilege Vulnerability	Important
Microsoft Windows Search Component	CVE-2020-0623	Windows Search Indexer Elevation of Privilege Vulnerability	Important
Microsoft Windows Search Component	CVE-2020-0625	Windows Search Indexer Elevation of Privilege Vulnerability	Important
Microsoft Windows Search Component	CVE-2020-0626	Windows Search Indexer Elevation of Privilege Vulnerability	Important
Microsoft Windows Search Component	CVE-2020-0627	Windows Search Indexer Elevation of Privilege Vulnerability	Important

Microsoft Windows Search Component	CVE-2020-0628	Windows Search Indexer Elevation of Privilege Vulnerability	Important
Microsoft Windows Search Component	CVE-2020-0629	Windows Search Indexer Elevation of Privilege Vulnerability	Important
Microsoft Windows Search Component	CVE-2020-0630	Windows Search Indexer Elevation of Privilege Vulnerability	Important
Microsoft Windows Search Component	CVE-2020-0631	Windows Search Indexer Elevation of Privilege Vulnerability	Important
Microsoft Windows Search Component	CVE-2020-0632	Windows Search Indexer Elevation of Privilege Vulnerability	Important
Microsoft Windows Search Component	CVE-2020-0633	Windows Search Indexer Elevation of Privilege Vulnerability	Important

Windows Hyper-V	CVE-2020-0617	Hyper-V Denial of service vulnerability	Important
Windows Media	CVE-2020-0641	Microsoft Windows Elevation of Privilege Vulnerability	Important
Windows RDP	CVE-2020-0609	Windows Remote Desktop Gateway (RD Gateway) Remote code execution vulnerability	Critical
Windows RDP	CVE-2020-0610	Windows Remote Desktop Gateway (RD Gateway) Remote code execution vulnerability	Critical
Windows RDP	CVE-2020-0611	Remote Desktop Client Remote code execution vulnerability	Critical
Windows RDP	CVE-2020-0612	Windows Remote Desktop Gateway (RD Gateway) Denial of service vulnerability	Important

Windows RDP	CVE-2020-0637	Remote Desktop Web Access Information Disclosure Vulnerability	Important
Windows Subsystem for Linux	CVE-2020-0636	Windows Subsystem for Linux Elevation of Privilege Vulnerability	Important
Windows Update Stack	CVE-2020-0638	Update Notification Manager Elevation of Privilege Vulnerability	Important

Recommended Mitigation Measures

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

Appendix

CVE-2020-0601 - Windows CryptoAPI Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0601 MITRE NVD	**CVE Title:** Windows CryptoAPI Spoofing Vulnerability **Description:** A spoofing vulnerability exists in the way Windows CryptoAPI (Crypt32.dll) validates Elliptic Curve Cryptography (ECC) certificates. An attacker could exploit the vulnerability by using a spoofed code-signing certificate to sign a malicious executable, making it appear the file was from a trusted, legitimate source. The user would have no way of knowing the file was malicious, because the digital signature would appear to be from a trusted provider. A successful exploit could also allow the attacker to conduct man-in-the-middle attacks and decrypt confidential information on user connections to the affected software. The security update addresses the vulnerability by ensuring that Windows CryptoAPI completely validates ECC certificates.	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: **Is there more information from Microsoft regarding CVE-2020-0601?** Yes, please see the blog post release on 1/14/2020. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published. 1.1 01/14/2020 08:00:00 Added an FAQ. This is an information change only.		

Affected Software

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

CVE-2020-0601						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Spoofing	4530717	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1803 for x64-based Systems	4534293 Security Update	Important	Spoofing	4530717	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows Server, version 1803 (Server	4534293 Security Update	Important	Spoofing	4530717	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-0601						
Core Installation)						
Windows 10 Version 1803 for ARM64-based Systems	4534293 Security Update	Important	Spoofing	4530717	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for 32-bit Systems	4534273 Security Update	Important	Spoofing	4530715	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for x64-based Systems	4534273 Security Update	Important	Spoofing	4530715	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for ARM64-	4534273 Security Update	Important	Spoofing	4530715	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-0601						
based Systems						
Windows Server 2019	4534273 Security Update	Important	Spoofing	4530715	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4534273 Security Update	Important	Spoofing	4530715	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1709 for 32-bit Systems	4534276 Security Update	Important	Spoofing	4530714	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1709 for x64-based Systems	4534276 Security Update	Important	Spoofing	4530714	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version	4534276 Security	Important	Spoofing	4530714	Base: 8.1 Temporal: 7.3	Unknown

CVE-2020-0601						
1709 for ARM64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1903 for 32-bit Systems	4528760 Security Update	Important	Spoofing	4530684	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4528760 Security Update	Important	Spoofing	4530684	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4528760 Security Update	Important	Spoofing	4530684	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version	4528760 Security	Important	Spoofing	4530684	Base: 8.1 Temporal: 7.3	Yes

CVE-2020-0601						
1903 (Server Core installation)	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	
Windows 10 for 32-bit Systems	4534306 Security Update	Important	Spoofing	4530681	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 for x64-based Systems	4534306 Security Update	Important	Spoofing	4530681	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for 32-bit Systems	4534271 Security Update	Important	Spoofing	4530689	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4534271 Security Update	Important	Spoofing	4530689	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-0601						
Windows Server 2016	4534271 Security Update	Important	Spoofing	4530689	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4534271 Security Update	Important	Spoofing	4530689	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1909 for 32-bit Systems	4528760 Security Update	Important	Spoofing	4530684	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4528760 Security Update	Important	Spoofing	4530684	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1909	4528760 Security Update	Important	Spoofing	4530684	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-0601						
(Server Core installation)						
Windows 10 Version 1909 for ARM64-based Systems	4528760 Security Update	Important	Spoofing	4530684	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-0602 - ASP.NET Core Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0602 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 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0602						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
ASP.NET Core 2.1	Release Notes Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
ASP.NET Core 3.0	Release Notes Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
ASP.NET Core 3.1	Rekease Notes Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0603 - ASP.NET Core Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0603 MITRE NVD	**CVE Title:** ASP.NET Core Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in ASP.NET Core software when the software fails to handle objects in memory.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of ASP.NET Core. 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. The security update addresses the vulnerability by correcting how ASP.NET Core handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0603						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
ASP.NET Core 2.1	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe
ASP.NET Core 3.0	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0603						
ASP.NET Core 3.1	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0605 - .NET Framework Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0605 MITRE NVD	**CVE Title:** .NET Framework Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in .NET software when the software fails to check the source markup of a 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. 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. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of .NET Framework. In an email attack scenario, an attacker could	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. The security update addresses the vulnerability by correcting how .NET Framework checks the source markup of a file. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0605						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
.NET Core 3.0	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe
.NET Core 3.1	Release Notes Security Update	Critical	Remote Code Execution		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	4535104 Monthly Rollup	Critical	Remote Code Execution	4524743; 4533097	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	4535104 Monthly Rollup 4534978 Security	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0605						
	Only					
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2	4535105 Monthly Rollup 4534979 Security Only	Critical	Remote Code Execution	4524744; 4533098	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	4535105 Monthly Rollup 4534979 Security Only	Critical	Remote Code Execution	4524744; 4533098	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	4535105 Monthly Rollup 4534979 Security Only	Critical	Remote Code Execution	4524744; 4533098	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0605						
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1909 for 32-bit Systems	4532938 Security Update	Critical	Remote Code Execution	4524744; 4533098	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)	4532938 Security Update	Critical	Remote Code Execution	4524744; 4533098	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	4532938 Security Update	Critical	Remote Code Execution	4524744; 4533098	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server, version 1803 (Server Core Installation)	4534293 Security Update	Critical	Remote Code Execution	4530717	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 for 32-bit Systems	4534306 Security	Critical	Remote Code Execution	4530681	Base: N/A Temporal: N/A	Unknown

CVE-2020-0605						
	Update				Vector: N/A	
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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	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 32-bit systems	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0605						
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	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)	4535103 Monthly Rollup 4534977 Security Only	Critical	Remote Code Execution	4524742; 4533096	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	4535103 Monthly Rollup 4534977 Security Only	Critical	Remote Code Execution	4524742; 4533096	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0605						
Microsoft .NET Framework 4.8 on Windows Server, version 1803 (Server Core Installation)	4532936 Security Update	Critical	Remote Code Execution	4524742; 4533096	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for 32-bit Systems	4534271 Security Update	Critical	Remote Code Execution	4530689	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for 32-bit Systems	4532936 Security Update	Critical	Remote Code Execution	4530689	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 (Server Core installation)	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0605						
Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for 32-bit Systems	4532935 Security Update	Critical	Remote Code Execution	4524741; 4533095	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 (Server Core installation)	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for x64-based Systems	4532936 Security Update	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A	Maybe

CVE-2020-0605						
					Vector: N/A	
Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for x64-based Systems	4532935 Security Update	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 R2 (Server Core installation)	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2016 (Server Core installation)	4532933 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012	4535103 Monthly Rollup 4534977	Critical	Remote Code Execution	4524742; 4533096	Base: N/A Temporal: N/A	Maybe

CVE-2020-0605						
	Security Only				Vector: N/A	
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for x64-based Systems	4532933 Security Update	Critical	Remote Code Execution	4524742; 4533096	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 R2	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server 2019	4535101 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2	4535105 Monthly Rollup	Critical	Remote Code Execution	4524744; 4533098	Base: N/A Temporal: N/A	Maybe

CVE-2020-0605						
	4534979 Security Only				Vector: N/A	
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1809 for 32-bit Systems	4535101 Security Update	Critical	Remote Code Execution	4524744; 4533098	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server 2019	4535101 Security Update	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0605						
Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for 32-bit Systems	4532933 Security Update	Critical	Remote Code Execution	4524741; 4533095	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)	4535101 Security Update	Critical	Remote Code Execution	4524741; 4533095	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)	4535101 Security Update	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0605						
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server, version 1903 (Server Core installation)	4532938 Security Update	Critical	Remote Code Execution	4524741; 4533095	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)	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 8.1 for 32-bit systems	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2016	4532933 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A	Maybe

CVE-2020-0605						
					Vector: N/A	
Microsoft .NET Framework 4.8 on Windows RT 8.1	4535104 Monthly Rollup	Critical	Remote Code Execution	4524743; 4533097	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	4535101 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 (Server Core installation)	4535103 Monthly Rollup 4534977 Security Only	Critical	Remote Code Execution	4524742; 4533096	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	4532938 Security Update	Critical	Remote Code Execution	4524742; 4533096	Base: N/A Temporal: N/A	Maybe

CVE-2020-0605						
					Vector: N/A	
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1809 for 32-bit Systems	4535101 Security Update	Critical	Remote Code Execution	4524742; 4533096	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	4535101 Security Update	Critical	Remote Code Execution	4524742; 4533096	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	4532938 Security Update	Critical	Remote Code Execution	4524742; 4533096	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	4535105 Monthly Rollup 4534979 Security	Critical	Remote Code Execution	4524744; 4533098	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0605						
	Only					
Microsoft .NET Framework 4.8 on Windows 7 for 32-bit Systems Service Pack 1	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 8.1 for x64-based systems	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0605						
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows RT 8.1	4535104 Monthly Rollup	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation)	4535104 Monthly Rollup 4534978	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A	Maybe

CVE-2020-0605						
	Security Only				Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012	4535103 Monthly Rollup 4534977 Security Only	Critical	Remote Code Execution	4524742; 4533096	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation)	4535103 Monthly Rollup 4534977 Security	Critical	Remote Code Execution	4524742; 4533096	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0605						
	Only					
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4535105 Monthly Rollup 4534979 Security Only	Critical	Remote Code Execution	4524744; 4533098	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0605						
Microsoft .NET Framework 4.5.2 on Windows 7 for 32-bit Systems Service Pack 1	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	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)	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0605						
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0605						
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation)	4535103 Monthly Rollup 4534977 Security Only	Critical	Remote Code Execution	4524742; 4533096	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation)	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0605						
Microsoft .NET Framework 4.5.2 on Windows Server 2012	4535103 Monthly Rollup 4534977 Security Only	Critical	Remote Code Execution	4524742; 4533096	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	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	4535105 Monthly Rollup 4534979 Security Only	Critical	Remote Code Execution	4524744; 4533098	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0605						
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	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	4534293 Security Update	Critical	Remote Code Execution	4530717	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1803 for x64-based Systems	4534293 Security Update	Critical	Remote Code Execution	4530717	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 for x64-based Systems	4534306 Security Update	Critical	Remote Code Execution	4530681	Base: N/A Temporal: N/A Vector: N/A	Unknown

CVE-2020-0605						
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	4534271 Security Update	Critical	Remote Code Execution	4530689	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 3.5 AND 4.7.1/4.7.2 on Windows 10 Version 1709 for 32-bit Systems	4534276 Security Update	Critical	Remote Code Execution	4530714	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	4534271 Security Update	Critical	Remote Code Execution	4530689	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)	4534271 Security Update	Critical	Remote Code Execution	4530689	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	4534271 Security	Critical	Remote Code Execution	4530689	Base: N/A Temporal: N/A	Unknown

CVE-2020-0605						
	Update				Vector: N/A	
Microsoft .NET Framework 3.5 AND 4.7.1/4.7.2 on Windows 10 Version 1709 for x64-based Systems	4534276 Security Update	Critical	Remote Code Execution	4530714	Base: N/A Temporal: N/A Vector: N/A	Unknown

CVE-2020-0606 - .NET Framework Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0606 MITRE NVD	**CVE Title:** .NET Framework Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in .NET software when the software fails to check the source markup of a 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of .NET Framework. 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. The security update addresses the vulnerability by correcting how .NET Framework checks the source markup of a file. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0606						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
.NET Core 3.0	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe
.NET Core 3.1	Release Notes Security Update	Critical	Remote Code Execution		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	4535102 Monthly Rollup 4534976 Security	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0606						
	Only					
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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	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 32-bit systems	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	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	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0606						
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows RT 8.1	4535104 Monthly Rollup	Critical	Remote Code Execution	4524743; 4533097	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	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 (Server Core installation)	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	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	4535103 Monthly Rollup 4534977	Critical	Remote Code Execution	4524742; 4533096	Base: N/A Temporal: N/A	Maybe

CVE-2020-0606						
	Security Only				Vector: N/A	
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)	4535103 Monthly Rollup 4534977 Security Only	Critical	Remote Code Execution	4524742; 4533096	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	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	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 (Server Core installation)	4535104 Monthly Rollup 4534978 Security	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0606						
	Only					
Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for 32-bit Systems	4532936 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for x64-based Systems	4532936 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server, version 1803 (Server Core Installation)	4532936 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for 32-bit Systems	4532935 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0606						
Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for x64-based Systems	4532935 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for 32-bit Systems	4532933 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for x64-based Systems	4532933 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2016	4532933 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2016 (Server Core installation)	4532933 Security	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A	Maybe

CVE-2020-0606						
	Update				Vector: N/A	
Microsoft .NET Framework 4.8 on Windows 7 for 32-bit Systems Service Pack 1	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 8.1 for 32-bit systems	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0606						
Microsoft .NET Framework 4.8 on Windows 8.1 for x64-based systems	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows RT 8.1	4535104 Monthly Rollup	Critical	Remote Code Execution	4524743; 4533097	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	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)	4535102 Monthly Rollup 4534976	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A	Maybe

CVE-2020-0606						
	Security Only				Vector: N/A	
Microsoft .NET Framework 4.8 on Windows Server 2012	4535103 Monthly Rollup 4534977 Security Only	Critical	Remote Code Execution	4524742; 4533096	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 (Server Core installation)	4535103 Monthly Rollup 4534977 Security Only	Critical	Remote Code Execution	4524742; 4533096	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 R2	4535104 Monthly Rollup 4534978 Security	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0606						
	Only					
Microsoft .NET Framework 4.8 on Windows Server 2012 R2 (Server Core installation)	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1809 for 32-bit Systems	4535101 Security Update	Critical	Remote Code Execution	4524743; 4533097	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	4535101 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server 2019	4535101 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A	Maybe

CVE-2020-0606						
					Vector: N/A	
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server 2019 (Server Core installation)	4535101 Security Update	Critical	Remote Code Execution	4524743; 4533097	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	4532938 Security Update	Critical	Remote Code Execution	4524743; 4533097	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	4532938 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server, version 1903 (Server Core installation)	4532938 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0606						
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1809 for 32-bit Systems	4535101 Security Update	Critical	Remote Code Execution	4524743; 4533097	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	4535101 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server 2019	4535101 Security Update	Critical	Remote Code Execution	4524743; 4533097	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)	4535101 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2	4535105 Monthly Rollup	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A	Maybe

CVE-2020-0606						
	4534979 Security Only				Vector: N/A	
Microsoft .NET Framework 4.6 on Windows Server 2008 for x64-based Systems Service Pack 2	4535105 Monthly Rollup 4534979 Security Only	Critical	Remote Code Execution	4524743; 4533097	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	4535105 Monthly Rollup 4534979 Security Only	Critical	Remote Code Execution	4524743; 4533097	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	4535105 Monthly Rollup 4534979 Security	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0606						
	Only					
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2	4535105 Monthly Rollup 4534979 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for 32-bit Systems	4534271 Security Update	Critical	Remote Code Execution	4530689	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0606						
Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012	4535103 Monthly Rollup 4534977 Security Only	Critical	Remote Code Execution	4524742; 4533096	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation)	4535103 Monthly Rollup 4534977 Security Only	Critical	Remote Code Execution	4524742; 4533096	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0606						
Microsoft .NET Framework 3.5 on Windows Server 2012 R2	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation)	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0606						
Microsoft .NET Framework 3.5.1 on Windows 7 for x64-based Systems Service Pack 1	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0606						
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0606						
Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows RT 8.1	4535104 Monthly Rollup	Critical	Remote Code Execution	4524743; 4533097	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	4535105 Monthly Rollup 4534979	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A	Maybe

CVE-2020-0606						
	Security Only				Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for x64-based Systems Service Pack 2	4535105 Monthly Rollup 4534979 Security Only	Critical	Remote Code Execution	4524743; 4533097	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	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)	4535102 Monthly Rollup 4534976 Security	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0606						
	Only					
Microsoft .NET Framework 4.5.2 on Windows Server 2012	4535103 Monthly Rollup 4534977 Security Only	Critical	Remote Code Execution	4524742; 4533096	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation)	4535103 Monthly Rollup 4534977 Security Only	Critical	Remote Code Execution	4524742; 4533096	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0606						
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation)	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1909 for 32-bit Systems	4532938 Security Update	Critical	Remote Code Execution	4524743; 4533097	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	4532938 Security Update	Critical	Remote Code Execution	4524743; 4533097	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)	4532938 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0606						
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 for x64-based Systems	4534306 Security Update	Critical	Remote Code Execution	4530681	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server, version 1803 (Server Core Installation)	4534293 Security Update	Critical	Remote Code Execution	4530717	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 32-bit Systems	4534271 Security Update	Critical	Remote Code Execution	4530689	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	4534271 Security Update	Critical	Remote Code Execution	4530689	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 3.5 AND 4.7.1/4.7.2 on Windows 10 Version 1709 for x64-based Systems	4534276 Security	Critical	Remote Code Execution	4530714	Base: N/A Temporal: N/A	Unknown

CVE-2020-0606						
	Update				Vector: N/A	
Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016	4534271 Security Update	Critical	Remote Code Execution	4530689	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 3.5 AND 4.7.1/4.7.2 on Windows 10 Version 1709 for 32-bit Systems	4534276 Security Update	Critical	Remote Code Execution	4530714	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)	4534271 Security Update	Critical	Remote Code Execution	4530689	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 for 32-bit Systems	4534306 Security Update	Critical	Remote Code Execution	4530681	Base: N/A Temporal: N/A Vector: N/A	Unknown

CVE-2020-0606						
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Critical	Remote Code Execution	4530717	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1803 for x64-based Systems	4534293 Security Update	Critical	Remote Code Execution	4530717	Base: N/A Temporal: N/A Vector: N/A	Unknown

CVE-2020-0607 - Microsoft Graphics Components Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0607	**CVE Title:** Microsoft Graphics Components Information Disclosure Vulnerability **Description:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	An information disclosure vulnerability exists in the way that Microsoft Graphics Components handle objects in memory. An attacker who successfully exploited the vulnerability could obtain information that could be useful for further exploitation. 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:** **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 01/14/2020 08:00:00 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-2020-0607						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Information Disclosure	4530717	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 1803 for x64-based Systems	4534293 Security Update	Important	Information Disclosure	4530717	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-2020-0607						
Windows Server, version 1803 (Server Core Installation)	4534293 Security Update	Important	Information Disclosure	4530717	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 1803 for ARM64-based Systems	4534293 Security Update	Important	Information Disclosure	4530717	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 32-bit Systems	4534273 Security Update	Important	Information Disclosure	4530715	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	4534273 Security Update	Important	Information Disclosure	4530715	Base: 5.5 Temporal: 5 Vector:	Unknown

CVE-2020-0607						
x64-based Systems					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 ARM64-based Systems	4534273 Security Update	Important	Information Disclosure	4530715	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	4534273 Security Update	Important	Information Disclosure	4530715	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)	4534273 Security Update	Important	Information Disclosure	4530715	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 1709 for	4534276 Security Update	Important	Information Disclosure	4530714	Base: 5.5 Temporal: 5 Vector:	Unknown

CVE-2020-0607						
32-bit Systems					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	4534276 Security Update	Important	Information Disclosure	4530714	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 1709 for ARM64-based Systems	4534276 Security Update	Important	Information Disclosure	4530714	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 1903 for 32-bit Systems	4528760 Security Update	Important	Information Disclosure	4530684	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	4528760 Security Update	Important	Information Disclosure	4530684	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-2020-0607						
Windows 10 Version 1903 for ARM64-based Systems	4528760 Security Update	Important	Information Disclosure	4530684	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)	4528760 Security Update	Important	Information Disclosure	4530684	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	4534306 Security Update	Important	Information Disclosure	4530681	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 for x64-based Systems	4534306 Security Update	Important	Information Disclosure	4530681	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-2020-0607						
Windows 10 Version 1607 for 32-bit Systems	4534271 Security Update	Important	Information Disclosure	4530689	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	4534271 Security Update	Important	Information Disclosure	4530689	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	4534271 Security Update	Important	Information Disclosure	4530689	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)	4534271 Security Update	Important	Information Disclosure	4530689	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	4534310 Monthly	Important	Information Disclosure	4530734	Base: 5.5 Temporal: 5	Yes

CVE-2020-0607						
Systems Service Pack 1	Rollup 4534314 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 7 for x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Information Disclosure	4530734	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 32-bit systems	4534297 Monthly Rollup 4534309 Security Only	Important	Information Disclosure	4530702	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 8.1 for x64-based systems	4534297 Monthly Rollup 4534309	Important	Information Disclosure	4530702	Base: 5.5 Temporal: 5 Vector:	Unknown

CVE-2020-0607						
	Security Only				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 2008 R2 for Itanium-Based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Information Disclosure	4530734	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 2008 R2 for x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Information Disclosure	4530734	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 2008 R2 for x64-based Systems	4534310 Monthly Rollup 4534314 Security	Important	Information Disclosure	4530734	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-2020-0607						
Service Pack 1 (Server Core installation)	Only					
Windows Server 2012	4534283 Monthly Rollup 4534288 Security Only	Important	Information Disclosure	4530691	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 (Server Core installation)	4534283 Monthly Rollup 4534288 Security Only	Important	Information Disclosure	4530691	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 R2	4534297 Monthly Rollup 4534309	Important	Information Disclosure	4530702	Base: 5.5 Temporal: 5 Vector:	Unknown

CVE-2020-0607						
	Security Only				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 2012 R2 (Server Core installation)	4534297 Monthly Rollup 4534309 Security Only	Important	Information Disclosure	4530702	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	4528760 Security Update	Important	Information Disclosure	4530684	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	4528760 Security Update	Important	Information Disclosure	4530684	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	4528760 Security	Important	Information Disclosure	4530684	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2020-0607						
ARM64-based Systems	Update				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 1909 (Server Core installation)	4528760 Security Update	Important	Information Disclosure	4530684	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-2020-0608 - Win32k Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0608 MITRE NVD	**CVE Title:** Win32k Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the win32k component improperly provides kernel information. 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
	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 win32k 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 uninitialized memory and kernel memory - unintentional read access to memory contents in kernel space from a user mode process. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0608						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Information Disclosure	4530717	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 1803 for x64-based Systems	4534293 Security Update	Important	Information Disclosure	4530717	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, version 1803 (Server Core	4534293 Security Update	Important	Information Disclosure	4530717	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-2020-0608						
Installation)						
Windows 10 Version 1803 for ARM64-based Systems	4534293 Security Update	Important	Information Disclosure	4530717	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 32-bit Systems	4534273 Security Update	Important	Information Disclosure	4530715	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	4534273 Security Update	Important	Information Disclosure	4530715	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-	4534273 Security Update	Important	Information Disclosure	4530715	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-2020-0608						
based Systems						
Windows Server 2019	4534273 Security Update	Important	Information Disclosure	4530715	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)	4534273 Security Update	Important	Information Disclosure	4530715	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 1709 for 32-bit Systems	4534276 Security Update	Important	Information Disclosure	4530714	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 1709 for x64-based Systems	4534276 Security Update	Important	Information Disclosure	4530714	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-2020-0608						
Windows 10 Version 1709 for ARM64-based Systems	4534276 Security Update	Important	Information Disclosure	4530714	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 1903 for 32-bit Systems	4528760 Security Update	Important	Information Disclosure	4530684	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	4528760 Security Update	Important	Information Disclosure	4530684	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	4528760 Security Update	Important	Information Disclosure	4530684	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-2020-0608						
Windows Server, version 1903 (Server Core installation)	4528760 Security Update	Important	Information Disclosure	4530684	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	4534306 Security Update	Important	Information Disclosure	4530681	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 for x64-based Systems	4534306 Security Update	Important	Information Disclosure	4530681	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 32-bit Systems	4534271 Security Update	Important	Information Disclosure	4530689	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-2020-0608						
Windows 10 Version 1607 for x64-based Systems	4534271 Security Update	Important	Information Disclosure	4530689	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	4534271 Security Update	Important	Information Disclosure	4530689	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)	4534271 Security Update	Important	Information Disclosure	4530689	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	4534310 Monthly Rollup 4534314 Security Only	Important	Information Disclosure	4530734	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-2020-0608						
Windows 7 for x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Information Disclosure	4530734	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 32-bit systems	4534297 Monthly Rollup 4534309 Security Only	Important	Information Disclosure	4530702	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 8.1 for x64-based systems	4534297 Monthly Rollup 4534309 Security Only	Important	Information Disclosure	4530702	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 RT 8.1	4534297 Monthly	Important	Information Disclosure	4530702	Base: 5.5 Temporal: 5	Unknown

CVE-2020-0608						
	Rollup				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 2008 for 32-bit Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Information Disclosure	4530695	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 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4534303 Monthly Rollup 4534312 Security Only	Important	Information Disclosure	4530695	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 2008 for	4534303 Monthly Rollup	Important	Information Disclosure	4530695	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2020-0608						
Itanium-Based Systems Service Pack 2	4534312 Security Only				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 2008 for x64-based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Information Disclosure	4530695	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 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4534303 Monthly Rollup 4534312 Security Only	Important	Information Disclosure	4530695	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-2020-0608						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Information Disclosure	4530734	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 2008 R2 for x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Information Disclosure	4530734	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 2008 R2 for x64-based Systems Service Pack 1 (Server	4534310 Monthly Rollup 4534314 Security Only	Important	Information Disclosure	4530734	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-2020-0608						
Core installation)						
Windows Server 2012	4534283 Monthly Rollup 4534288 Security Only	Important	Information Disclosure	4530691	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 (Server Core installation)	4534283 Monthly Rollup 4534288 Security Only	Important	Information Disclosure	4530691	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 R2	4534297 Monthly Rollup 4534309 Security Only	Important	Information Disclosure	4530702	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-2020-0608						
Windows Server 2012 R2 (Server Core installation)	4534297 Monthly Rollup 4534309 Security Only	Important	Information Disclosure	4530702	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	4528760 Security Update	Important	Information Disclosure	4530684	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	4528760 Security Update	Important	Information Disclosure	4530684	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	4528760 Security Update	Important	Information Disclosure	4530684	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-2020-0608						
Windows Server, version 1909 (Server Core installation)	4528760 Security Update	Important	Information Disclosure	4530684	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-2020-0609 - Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0609 MITRE NVD	**CVE Title:** Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target 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 send a specially crafted request to the target systems RD Gateway via RDP. The update addresses the vulnerability by correcting how RD Gateway handles connection requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0609						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2019	4534273 Security Update	Critical	Remote Code Execution	4530715	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4534271 Security Update	Critical	Remote Code Execution	4530689	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2012	4534283 Monthly Rollup 4534288 Security Only	Critical	Remote Code Execution	4530691	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0609						
Windows Server 2012 R2	4534297 Monthly Rollup 4534309 Security Only	Critical	Remote Code Execution	4530702	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0610 - Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0610 MITRE NVD	**CVE Title:** Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target 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 send a specially crafted request to the target systems RD Gateway via RDP. The update addresses the vulnerability by correcting how RD Gateway handles connection requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0610						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2019	4534273 Security Update	Critical	Remote Code Execution	4530715	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016	4534271 Security Update	Critical	Remote Code Execution	4530689	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2012	4534283 Monthly Rollup 4534288 Security Only	Critical	Remote Code Execution	4530691	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0610						
Windows Server 2012 R2	4534297 Monthly Rollup 4534309 Security Only	Critical	Remote Code Execution	4530702	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0611 - Remote Desktop Client Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0611 MITRE NVD	**CVE Title:** Remote Desktop Client Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server. An attacker who successfully exploited this vulnerability could execute arbitrary code on the computer of the connecting client. An	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 have control of a server and then convince a user to connect to it. An attacker would have no way of forcing a user to connect to the malicious server, they would need to trick the user into connecting via social engineering, DNS poisoning or using a Man in the Middle (MITM) technique. An attacker could also compromise a legitimate server, host malicious code on it, and wait for the user to connect. The update addresses the vulnerability by correcting how the Windows Remote Desktop Client handles connection requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 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-2020-0611						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Critical	Remote Code Execution	4530717	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 1803 for x64-based Systems	4534293 Security Update	Critical	Remote Code Execution	4530717	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-2020-0611						
Windows Server, version 1803 (Server Core Installation)	4534293 Security Update	Critical	Remote Code Execution	4530717	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 1803 for ARM64-based Systems	4534293 Security Update	Critical	Remote Code Execution	4530717	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 32-bit Systems	4534273 Security Update	Critical	Remote Code Execution	4530715	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	4534273 Security Update	Critical	Remote Code Execution	4530715	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-2020-0611						
Windows 10 Version 1809 for ARM64-based Systems	4534273 Security Update	Critical	Remote Code Execution	4530715	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	4534273 Security Update	Critical	Remote Code Execution	4530715	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 (Server Core installation)	4534273 Security Update	Critical	Remote Code Execution	4530715	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 1709 for 32-bit Systems	4534276 Security Update	Critical	Remote Code Execution	4530714	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 1709 for	4534276 Security	Critical	Remote Code Execution	4530714	Base: 7.5 Temporal: 6.7	Unknown

CVE-2020-0611						
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	
Windows 10 Version 1709 for ARM64-based Systems	4534276 Security Update	Critical	Remote Code Execution	4530714	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 1903 for 32-bit Systems	4528760 Security Update	Critical	Remote Code Execution	4530684	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	4528760 Security Update	Critical	Remote Code Execution	4530684	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-	4528760 Security Update	Critical	Remote Code Execution	4530684	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-2020-0611						
based Systems						
Windows Server, version 1903 (Server Core installation)	4528760 Security Update	Critical	Remote Code Execution	4530684	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 32-bit Systems	4534306 Security Update	Critical	Remote Code Execution	4530681	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 for x64-based Systems	4534306 Security Update	Critical	Remote Code Execution	4530681	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 32-bit Systems	4534271 Security Update	Critical	Remote Code Execution	4530689	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-2020-0611						
Windows 10 Version 1607 for x64-based Systems	4534271 Security Update	Critical	Remote Code Execution	4530689	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	4534271 Security Update	Critical	Remote Code Execution	4530689	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 (Server Core installation)	4534271 Security Update	Critical	Remote Code Execution	4530689	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 32-bit Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Critical	Remote Code Execution	4530734	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-2020-0611						
Windows 7 for x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Critical	Remote Code Execution	4530734	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 8.1 for 32-bit systems	4534297 Monthly Rollup 4534309 Security Only	Critical	Remote Code Execution	4530702	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 x64-based systems	4534297 Monthly Rollup 4534309 Security Only	Critical	Remote Code Execution	4530702	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-2020-0611						
Windows RT 8.1	4534297 Monthly Rollup	Critical	Remote Code Execution	4530702	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 2008 R2 for Itanium-Based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Critical	Remote Code Execution	4530734	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 R2 for x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Critical	Remote Code Execution	4530734	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 R2 for x64-based	4534310 Monthly Rollup 4534314	Critical	Remote Code Execution	4530734	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-2020-0611						
Systems Service Pack 1 (Server Core installation)	Security Only					
Windows Server 2012	4534283 Monthly Rollup 4534288 Security Only	Critical	Remote Code Execution	4530691	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 2012 (Server Core installation)	4534283 Monthly Rollup 4534288 Security Only	Critical	Remote Code Execution	4530691	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 2012 R2	4534297 Monthly Rollup	Critical	Remote Code Execution	4530702	Base: 7.5 Temporal: 6.7	Unknown

CVE-2020-0611						
	4534309 Security Only				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 2012 R2 (Server Core installation)	4534297 Monthly Rollup 4534309 Security Only	Critical	Remote Code Execution	4530702	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 1909 for 32-bit Systems	4528760 Security Update	Critical	Remote Code Execution	4530684	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	4528760 Security Update	Critical	Remote Code Execution	4530684	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-2020-0611						
Windows 10 Version 1909 for ARM64-based Systems	4528760 Security Update	Critical	Remote Code Execution	4530684	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)	4528760 Security Update	Critical	Remote Code Execution	4530684	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-2020-0612 - Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0612 MITRE NVD	**CVE Title:** Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability **Description:** A denial of service vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an attacker connects to the target system using RDP and sends specially crafted requests. An attacker who successfully exploited this vulnerability could cause the RD Gateway service on the target system to stop responding. To exploit this vulnerability, an attacker would need to run a specially crafted application against a server which provides RD Gateway services. The update addresses the vulnerability by correcting how RD Gateway handles connection requests. **FAQ:** None	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0612						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2019	4534273 Security	Important	Denial of Service	4530715	Base: 7.5 Temporal: 6.7	Unknown

CVE-2020-0612						
	Update				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	
Windows Server 2016	4534271 Security Update	Important	Denial of Service	4530689	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-2020-0613 - Windows Search Indexer Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0613 MITRE NVD	**CVE Title:** Windows Search Indexer Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way that the Windows Search Indexer 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.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by ensuring the Windows Search Indexer properly handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0613						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0613						
Windows 10 Version 1809 for 32-bit Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0613						
Windows 10 Version 1709 for 32-bit Systems	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 ARM64-based Systems	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 1903 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0613						
x64-based Systems						
Windows 10 Version 1903 for ARM64-based Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV: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	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 for x64-based Systems	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0613						
Windows 10 Version 1607 for 32-bit Systems	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534297 Monthly Rollup 4534309 Security	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0613						
	Only					
Windows 8.1 for x64-based systems	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4534297 Monthly Rollup	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 R2	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 R2 (Server	4534297 Monthly Rollup	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7	Unknown

CVE-2020-0613						
Core installation)	4534309 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 10 Version 1909 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0613						
(Server Core installation)						

CVE-2020-0614 - Windows Search Indexer Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0614 MITRE NVD	**CVE Title:** Windows Search Indexer Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way that the Windows Search Indexer 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 Search Indexer properly 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 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0614						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version	4534293 Security	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7	Unknown

CVE-2020-0614						
1803 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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0614						
Windows 10 Version 1809 for x64-based Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0614						
Windows 10 Version 1709 for x64-based Systems	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 ARM64-based Systems	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 1903 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7	Yes

CVE-2020-0614						
ARM64-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 1903 (Server Core installation)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV: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	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 for x64-based Systems	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0614						
Windows 10 Version 1607 for x64-based Systems	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-	4534297 Monthly Rollup	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7	Unknown

CVE-2020-0614						
based systems	4534309 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 RT 8.1	4534297 Monthly Rollup	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 R2	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 R2 (Server Core installation)	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0614						
Windows 10 Version 1909 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0615 - Windows Common Log File System Driver Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0615 MITRE NVD	**CVE Title:** Windows Common Log File System Driver Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could potentially read data that was not intended to be disclosed. Note that this vulnerability would not allow an attacker to execute code or to elevate their user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system. 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.	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 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 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0615						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Information Disclosure	4530717	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 1803 for x64-based Systems	4534293 Security Update	Important	Information Disclosure	4530717	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, version 1803 (Server Core Installation)	4534293 Security Update	Important	Information Disclosure	4530717	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 1803 for	4534293 Security	Important	Information Disclosure	4530717	Base: 5.5 Temporal: 5 Vector:	Unknown

CVE-2020-0615						
ARM64-based Systems	Update				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 32-bit Systems	4534273 Security Update	Important	Information Disclosure	4530715	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	4534273 Security Update	Important	Information Disclosure	4530715	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	4534273 Security Update	Important	Information Disclosure	4530715	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	4534273 Security Update	Important	Information Disclosure	4530715	Base: 5.5 Temporal: 5 Vector:	Unknown

CVE-2020-0615						
					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 (Server Core installation)	4534273 Security Update	Important	Information Disclosure	4530715	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 1709 for 32-bit Systems	4534276 Security Update	Important	Information Disclosure	4530714	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 1709 for x64-based Systems	4534276 Security Update	Important	Information Disclosure	4530714	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 1709 for ARM64-	4534276 Security Update	Important	Information Disclosure	4530714	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-2020-0615						
based Systems						
Windows 10 Version 1903 for 32-bit Systems	4528760 Security Update	Important	Information Disclosure	4530684	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	4528760 Security Update	Important	Information Disclosure	4530684	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	4528760 Security Update	Important	Information Disclosure	4530684	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	4528760 Security Update	Important	Information Disclosure	4530684	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-2020-0615						
Core installation)						
Windows 10 for 32-bit Systems	4534306 Security Update	Important	Information Disclosure	4530681	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 for x64-based Systems	4534306 Security Update	Important	Information Disclosure	4530681	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 32-bit Systems	4534271 Security Update	Important	Information Disclosure	4530689	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	4534271 Security Update	Important	Information Disclosure	4530689	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-2020-0615						
Windows Server 2016	4534271 Security Update	Important	Information Disclosure	4530689	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)	4534271 Security Update	Important	Information Disclosure	4530689	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	4534310 Monthly Rollup 4534314 Security Only	Important	Information Disclosure	4530734	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 7 for x64-based Systems	4534310 Monthly Rollup 4534314 Security	Important	Information Disclosure	4530734	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-2020-0615						
Service Pack 1	Only					
Windows 8.1 for 32-bit systems	4534297 Monthly Rollup 4534309 Security Only	Important	Information Disclosure	4530702	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 8.1 for x64-based systems	4534297 Monthly Rollup 4534309 Security Only	Important	Information Disclosure	4530702	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 RT 8.1	4534297 Monthly Rollup	Important	Information Disclosure	4530702	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	4534303 Monthly	Important	Information Disclosure	4530695	Base: 5.5 Temporal: 5	Yes

CVE-2020-0615						
2008 for 32-bit Systems Service Pack 2	Rollup 4534312 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 Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4534303 Monthly Rollup 4534312 Security Only	Important	Information Disclosure	4530695	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 2008 for Itanium-Based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Information Disclosure	4530695	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-2020-0615						
Windows Server 2008 for x64-based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Information Disclosure	4530695	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 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4534303 Monthly Rollup 4534312 Security Only	Important	Information Disclosure	4530695	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 2008 R2 for Itanium-Based Systems	4534310 Monthly Rollup 4534314 Security	Important	Information Disclosure	4530734	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-2020-0615						
Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Information Disclosure	4530734	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 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4534310 Monthly Rollup 4534314 Security Only	Important	Information Disclosure	4530734	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	4534283 Monthly Rollup 4534288	Important	Information Disclosure	4530691	Base: 5.5 Temporal: 5 Vector:	Unknown

CVE-2020-0615						
	Security Only				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 2012 (Server Core installation)	4534283 Monthly Rollup 4534288 Security Only	Important	Information Disclosure	4530691	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 R2	4534297 Monthly Rollup 4534309 Security Only	Important	Information Disclosure	4530702	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 R2 (Server Core installation)	4534297 Monthly Rollup 4534309 Security	Important	Information Disclosure	4530702	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-2020-0615						
	Only					
Windows 10 Version 1909 for 32-bit Systems	4528760 Security Update	Important	Information Disclosure	4530684	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	4528760 Security Update	Important	Information Disclosure	4530684	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	4528760 Security Update	Important	Information Disclosure	4530684	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	4528760 Security Update	Important	Information Disclosure	4530684	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-2020-0615						
Core installation)						

CVE-2020-0616 - Microsoft Windows Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0616 MITRE NVD	**CVE Title:** Microsoft Windows Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when Windows improperly handles hard links. 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 allow an attacker to overwrite system files. The update addresses the vulnerability by correcting ACLs to system files. **FAQ:** None **Mitigations:**	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0616						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1809 for 32-bit Systems	4534273 Security Update	Important	Denial of Service	4530715	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-2020-0616						
Windows 10 Version 1809 for x64-based Systems	4534273 Security Update	Important	Denial of Service	4530715	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	4534273 Security Update	Important	Denial of Service	4530715	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	4534273 Security Update	Important	Denial of Service	4530715	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)	4534273 Security Update	Important	Denial of Service	4530715	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 1903 for 32-bit Systems	4528760 Security Update	Important	Denial of Service	4530684	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-2020-0616						
Windows 10 Version 1903 for x64-based Systems	4528760 Security Update	Important	Denial of Service	4530684	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	4528760 Security Update	Important	Denial of Service	4530684	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)	4528760 Security Update	Important	Denial of Service	4530684	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 32-bit Systems	4528760 Security Update	Important	Denial of Service	4530684	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-	4528760 Security Update	Important	Denial of Service	4530684	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-2020-0616						
based Systems						
Windows 10 Version 1909 for ARM64-based Systems	4528760 Security Update	Important	Denial of Service	4530684	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)	4528760 Security Update	Important	Denial of Service	4530684	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-2020-0617 - Hyper-V Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0617	**CVE Title:** Hyper-V Denial of Service Vulnerability **Description:**	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A denial of service vulnerability exists when Microsoft Hyper-V Virtual PCI on a host server fails to properly validate input from a privileged user on a guest operating system. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application that causes a host machine to crash. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application. The security update addresses the vulnerability by properly validating input. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0617						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for x64-based Systems	4534293 Security Update	Important	Denial of Service	4530717	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows Server, version 1803 (Server Core Installation)	4534293 Security Update	Important	Denial of Service	4530717	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:H/PR:H/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	4534273 Security Update	Important	Denial of Service	4530715	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0617						
Windows Server 2019	4534273 Security Update	Important	Denial of Service	4530715	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4534273 Security Update	Important	Denial of Service	4530715	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1709 for x64-based Systems	4534276 Security Update	Important	Denial of Service	4530714	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 for x64-based Systems	4534306 Security Update	Important	Denial of Service	4530681	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1607 for x64-based Systems	4534271 Security Update	Important	Denial of Service	4530689	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0617						
Windows Server 2016	4534271 Security Update	Important	Denial of Service	4530689	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4534271 Security Update	Important	Denial of Service	4530689	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0620 - Microsoft Cryptographic Services Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0620 MITRE NVD	**CVE Title:** Microsoft Cryptographic Services Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft Cryptographic Services improperly handles files. An attacker could exploit the vulnerability to overwrite or modify a protected file leading to a privilege escalation.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, an attacker would first require execution on the victim system. The security update addresses the vulnerability by addressing how Microsoft Cryptographic Services handles files. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0620						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0620						
Windows 10 Version 1809 for 32-bit Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0620						
Windows 10 Version 1709 for 32-bit Systems	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 ARM64-based Systems	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 1903 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0620						
x64-based Systems						
Windows 10 Version 1903 for ARM64-based Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV: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	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 for x64-based Systems	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0620						
Windows 10 Version 1607 for 32-bit Systems	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534310 Monthly Rollup 4534314 Security	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0620						
	Only					
Windows 7 for x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit systems	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based systems	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0620						
Windows RT 8.1	4534297 Monthly Rollup	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 (Server Core installation)	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 Itanium-Based	4534303 Monthly Rollup 4534312	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0620						
Systems Service Pack 2	Security Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based Systems Service Pack 2 (Server Core installation)	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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-	4534310 Monthly Rollup 4534314	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0620						
Based Systems Service Pack 1	Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based Systems Service Pack 1 (Server Core installation)	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534283 Monthly Rollup	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7	Unknown

CVE-2020-0620						
	4534288 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)	4534283 Monthly Rollup 4534288 Security Only	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 R2	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 R2 (Server Core installation)	4534297 Monthly Rollup 4534309 Security	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0620						
	Only					
Windows 10 Version 1909 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0621 - Windows Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0621 MITRE NVD	**CVE Title:** Windows Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists in Windows 10 when third party filters are called during a password update. Successful exploitation of the vulnerability could allow a user to make use of a blocked password for their account. To exploit the vulnerability, an attacker would need have access and the current password for the target user. The update addresses how password filters are called during a password update. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00	Important	Security Feature Bypass

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-2020-0621						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Security Feature Bypass	4530717	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1803 for x64-based Systems	4534293 Security Update	Important	Security Feature Bypass	4530717	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-0621						
Windows Server, version 1803 (Server Core Installation)	4534293 Security Update	Important	Security Feature Bypass	4530717	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1803 for ARM64-based Systems	4534293 Security Update	Important	Security Feature Bypass	4530717	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1809 for 32-bit Systems	4534273 Security Update	Important	Security Feature Bypass	4530715	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/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	4534273 Security Update	Important	Security Feature Bypass	4530715	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-0621						
Windows 10 Version 1809 for ARM64-based Systems	4534273 Security Update	Important	Security Feature Bypass	4530715	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2019	4534273 Security Update	Important	Security Feature Bypass	4530715	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core installation)	4534273 Security Update	Important	Security Feature Bypass	4530715	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1709 for 32-bit Systems	4534276 Security Update	Important	Security Feature Bypass	4530714	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 Version 1709 for x64-based Systems	4534276 Security Update	Important	Security Feature Bypass	4530714	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-0621						
Windows 10 Version 1709 for ARM64-based Systems	4534276 Security Update	Important	Security Feature Bypass	4530714	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-0622 - Microsoft Graphics Component Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0622 MITRE NVD	**CVE Title:** Microsoft Graphics Component Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in 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
	To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The update addresses the vulnerability by correcting the way in which the Windows Graphics 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 uninitialized memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0622						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Information Disclosure	4530717	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 1803 for x64-based Systems	4534293 Security Update	Important	Information Disclosure	4530717	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, version 1803 (Server Core	4534293 Security Update	Important	Information Disclosure	4530717	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-2020-0622						
Installation)						
Windows 10 Version 1803 for ARM64-based Systems	4534293 Security Update	Important	Information Disclosure	4530717	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 1709 for 32-bit Systems	4534276 Security Update	Important	Information Disclosure	4530714	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 1709 for x64-based Systems	4534276 Security Update	Important	Information Disclosure	4530714	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 1709 for ARM64-	4534276 Security Update	Important	Information Disclosure	4530714	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-2020-0622						
based Systems						
Windows 10 for 32-bit Systems	4534306 Security Update	Important	Information Disclosure	4530681	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 for x64-based Systems	4534306 Security Update	Important	Information Disclosure	4530681	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 32-bit Systems	4534271 Security Update	Important	Information Disclosure	4530689	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	4534271 Security Update	Important	Information Disclosure	4530689	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-2020-0622						
Windows Server 2016	4534271 Security Update	Important	Information Disclosure	4530689	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)	4534271 Security Update	Important	Information Disclosure	4530689	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-2020-0623 - Windows Search Indexer Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0623	**CVE Title:** Windows Search Indexer 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 in the way that the Windows Search Indexer 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 Search Indexer properly handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0623						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0623						
Windows 10 Version 1803 for ARM64-based Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0623						
Windows Server 2019	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 ARM64-based Systems	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0623						
Windows 10 Version 1903 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0623						
Windows 10 for 32-bit Systems	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 for x64-based Systems	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0623						
Windows Server 2016 (Server Core installation)	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based systems	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4534297 Monthly Rollup	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0623						
Windows Server 2012 R2	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 R2 (Server Core installation)	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0623						
Windows 10 Version 1909 for ARM64-based Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0624 - Win32k Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0624	**CVE Title:** Win32k 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 in Windows when the Win32k component 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 Win32k handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0624						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1903 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0624						
Windows Server, version 1903 (Server Core installation)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0624						
Windows Server, version 1909 (Server Core installation)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0625 - Windows Search Indexer Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0625 MITRE NVD	**CVE Title:** Windows Search Indexer Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way that the Windows Search Indexer 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.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by ensuring the Windows Search Indexer properly handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0625						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0625						
Windows 10 Version 1809 for 32-bit Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0625						
Windows 10 Version 1709 for 32-bit Systems	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 ARM64-based Systems	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 1903 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0625						
x64-based Systems						
Windows 10 Version 1903 for ARM64-based Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV: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	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 for x64-based Systems	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0625						
Windows 10 Version 1607 for 32-bit Systems	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534310 Monthly Rollup 4534314 Security	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0625						
	Only					
Windows 7 for x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit systems	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based systems	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0625						
Windows RT 8.1	4534297 Monthly Rollup	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 (Server Core installation)	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 Itanium-Based	4534303 Monthly Rollup 4534312	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0625						
Systems Service Pack 2	Security Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based Systems Service Pack 2 (Server Core installation)	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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-	4534310 Monthly Rollup 4534314	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0625						
Based Systems Service Pack 1	Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based Systems Service Pack 1 (Server Core installation)	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534283 Monthly Rollup	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7	Unknown

CVE-2020-0625						
	4534288 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)	4534283 Monthly Rollup 4534288 Security Only	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 R2	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 R2 (Server Core installation)	4534297 Monthly Rollup 4534309 Security	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0625						
	Only					
Windows 10 Version 1909 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0626 - Windows Search Indexer Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0626 MITRE NVD	**CVE Title:** Windows Search Indexer Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way that the Windows Search Indexer 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 Search Indexer properly 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 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0626						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7	Unknown

CVE-2020-0626						
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)	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0626						
Windows 10 Version 1809 for ARM64-based Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0626						
Windows 10 Version 1709 for ARM64-based Systems	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 1903 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0626						
Windows Server, version 1903 (Server Core installation)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV: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	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 for x64-based Systems	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0626						
Windows Server 2016	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0626						
Windows 8.1 for 32-bit systems	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based systems	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4534297 Monthly Rollup	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534303 Monthly Rollup 4534312 Security	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0626						
Service Pack 2	Only					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 Itanium-Based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based Systems	4534303 Monthly Rollup 4534312 Security	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0626						
Service Pack 2	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based	4534310 Monthly Rollup 4534314	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0626						
Systems Service Pack 1	Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534283 Monthly Rollup 4534288 Security Only	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 (Server Core installation)	4534283 Monthly Rollup 4534288	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0626						
	Security Only					
Windows Server 2012 R2	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 R2 (Server Core installation)	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0626						
Windows 10 Version 1909 for x64-based Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0627 - Windows Search Indexer Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0627 MITRE NVD	**CVE Title:** Windows Search Indexer Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way that the Windows Search Indexer 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 Search Indexer properly 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 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0627						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7	Unknown

CVE-2020-0627						
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)	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0627						
Windows 10 Version 1809 for ARM64-based Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0627						
Windows 10 Version 1709 for ARM64-based Systems	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 1903 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0627						
Windows Server, version 1903 (Server Core installation)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV: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	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 for x64-based Systems	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0627						
Windows Server 2016	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0627						
Windows 8.1 for 32-bit systems	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based systems	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4534297 Monthly Rollup	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534303 Monthly Rollup 4534312 Security	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0627						
Service Pack 2	Only					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 Itanium-Based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based Systems	4534303 Monthly Rollup 4534312 Security	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0627						
Service Pack 2	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based	4534310 Monthly Rollup 4534314	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0627						
Systems Service Pack 1	Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534283 Monthly Rollup 4534288 Security Only	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 (Server Core installation)	4534283 Monthly Rollup 4534288	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0627						
	Security Only					
Windows Server 2012 R2	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 R2 (Server Core installation)	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0627						
Windows 10 Version 1909 for x64-based Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0628 - Windows Search Indexer Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0628 MITRE NVD	**CVE Title:** Windows Search Indexer Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way that the Windows Search Indexer 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 Search Indexer properly 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 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0628						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7	Unknown

CVE-2020-0628						
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)	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0628						
Windows 10 Version 1809 for ARM64-based Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0628						
Windows 10 Version 1709 for ARM64-based Systems	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 1903 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0628						
Windows Server, version 1903 (Server Core installation)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV: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	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 for x64-based Systems	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0628						
Windows Server 2016	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0628						
Windows 8.1 for 32-bit systems	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based systems	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4534297 Monthly Rollup	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534303 Monthly Rollup 4534312 Security	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0628						
Service Pack 2	Only					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 Itanium-Based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based Systems	4534303 Monthly Rollup 4534312 Security	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0628						
Service Pack 2	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based	4534310 Monthly Rollup 4534314	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0628						
Systems Service Pack 1	Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534283 Monthly Rollup 4534288 Security Only	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 (Server Core installation)	4534283 Monthly Rollup 4534288	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0628						
	Security Only					
Windows Server 2012 R2	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 R2 (Server Core installation)	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0628						
Windows 10 Version 1909 for x64-based Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0629 - Windows Search Indexer Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0629 MITRE NVD	**CVE Title:** Windows Search Indexer Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way that the Windows Search Indexer 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 Search Indexer properly 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 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0629						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7	Unknown

CVE-2020-0629						
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)	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0629						
Windows 10 Version 1809 for ARM64-based Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0629						
Windows 10 Version 1709 for ARM64-based Systems	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 1903 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0629						
Windows Server, version 1903 (Server Core installation)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV: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	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 for x64-based Systems	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0629						
Windows Server 2016	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0629						
Windows 8.1 for 32-bit systems	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based systems	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4534297 Monthly Rollup	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534303 Monthly Rollup 4534312 Security	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0629						
Service Pack 2	Only					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 Itanium-Based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based Systems	4534303 Monthly Rollup 4534312 Security	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0629						
Service Pack 2	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based	4534310 Monthly Rollup 4534314	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0629						
Systems Service Pack 1	Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534283 Monthly Rollup 4534288 Security Only	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 (Server Core installation)	4534283 Monthly Rollup 4534288	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0629						
	Security Only					
Windows Server 2012 R2	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 R2 (Server Core installation)	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0629						
Windows 10 Version 1909 for x64-based Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0630 - Windows Search Indexer Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0630 MITRE NVD	**CVE Title:** Windows Search Indexer Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way that the Windows Search Indexer 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 Search Indexer properly 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 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0630						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7	Unknown

CVE-2020-0630						
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)	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0630						
Windows 10 Version 1809 for ARM64-based Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 ARM64-	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0630						
based Systems						
Windows 10 Version 1903 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0630						
Windows 10 for 32-bit Systems	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 for x64-based Systems	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0630						
Windows Server 2016 (Server Core installation)	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit systems	4534297 Monthly Rollup 4534309 Security	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0630						
	Only					
Windows 8.1 for x64-based systems	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4534297 Monthly Rollup	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534303 Monthly Rollup	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7	Yes

CVE-2020-0630						
Systems Service Pack 2 (Server Core installation)	4534312 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 2008 for Itanium-Based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based	4534303 Monthly Rollup 4534312	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0630						
Systems Service Pack 2 (Server Core installation)	Security Only					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-	4534310 Monthly Rollup	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7	Yes

CVE-2020-0630						
based Systems Service Pack 1 (Server Core installation)	4534314 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	4534283 Monthly Rollup 4534288 Security Only	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 (Server Core installation)	4534283 Monthly Rollup 4534288 Security Only	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 R2	4534297 Monthly Rollup	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7	Unknown

CVE-2020-0630						
	4534309 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 R2 (Server Core installation)	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7	Yes

CVE-2020-0630						
ARM64-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 1909 (Server Core installation)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0631 - Windows Search Indexer Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0631 MITRE NVD	**CVE Title:** Windows Search Indexer 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 the way that the Windows Search Indexer 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 Search Indexer properly handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0631						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0631						
Windows 10 Version 1803 for ARM64-based Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0631						
Windows Server 2019	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 ARM64-based Systems	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0631						
Windows 10 Version 1903 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0631						
Windows 10 for 32-bit Systems	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 for x64-based Systems	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0631						
Windows Server 2016 (Server Core installation)	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit systems	4534297 Monthly Rollup 4534309 Security	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0631						
	Only					
Windows 8.1 for x64-based systems	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4534297 Monthly Rollup	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534303 Monthly Rollup	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7	Yes

CVE-2020-0631						
Systems Service Pack 2 (Server Core installation)	4534312 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 2008 for Itanium-Based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based	4534303 Monthly Rollup 4534312	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0631						
Systems Service Pack 2 (Server Core installation)	Security Only					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-	4534310 Monthly Rollup	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7	Yes

CVE-2020-0631						
based Systems Service Pack 1 (Server Core installation)	4534314 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	4534283 Monthly Rollup 4534288 Security Only	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 (Server Core installation)	4534283 Monthly Rollup 4534288 Security Only	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 R2	4534297 Monthly Rollup	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7	Unknown

CVE-2020-0631						
	4534309 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 R2 (Server Core installation)	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7	Yes

CVE-2020-0631						
ARM64-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 1909 (Server Core installation)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0632 - Windows Search Indexer Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0632 MITRE NVD	**CVE Title:** Windows Search Indexer 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 the way that the Windows Search Indexer 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 Search Indexer properly handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0632						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0632						
Windows 10 Version 1803 for ARM64-based Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0632						
Windows Server 2019	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 ARM64-based Systems	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0632						
Windows 10 Version 1903 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0632						
Windows 10 for 32-bit Systems	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 for x64-based Systems	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0632						
Windows Server 2016 (Server Core installation)	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit systems	4534297 Monthly Rollup 4534309 Security	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0632						
	Only					
Windows 8.1 for x64-based systems	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4534297 Monthly Rollup	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534303 Monthly Rollup	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7	Yes

CVE-2020-0632						
Systems Service Pack 2 (Server Core installation)	4534312 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 2008 for Itanium-Based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based	4534303 Monthly Rollup 4534312	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0632						
Systems Service Pack 2 (Server Core installation)	Security Only					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-	4534310 Monthly Rollup	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7	Yes

CVE-2020-0632						
based Systems Service Pack 1 (Server Core installation)	4534314 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	4534283 Monthly Rollup 4534288 Security Only	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 (Server Core installation)	4534283 Monthly Rollup 4534288 Security Only	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 R2	4534297 Monthly Rollup	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7	Unknown

CVE-2020-0632						
	4534309 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 R2 (Server Core installation)	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7	Yes

CVE-2020-0632						
ARM64-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 1909 (Server Core installation)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0633 - Windows Search Indexer Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0633 MITRE NVD	**CVE Title:** Windows Search Indexer 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 the way that the Windows Search Indexer 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 Search Indexer properly handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0633						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0633						
Windows 10 Version 1803 for ARM64-based Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0633						
Windows Server 2019	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 ARM64-based Systems	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0633						
Windows 10 Version 1903 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0633						
Windows 10 Version 1607 for 32-bit Systems	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0633						
Windows 10 Version 1909 for x64-based Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0634 - Windows Common Log File System Driver Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0634 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:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0634						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0634						
Windows 10 Version 1803 for x64-based Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0634						
Windows 10 Version 1809 for x64-based Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0634						
Windows 10 Version 1709 for x64-based Systems	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 ARM64-based Systems	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 1903 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7	Yes

CVE-2020-0634						
ARM64-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 1903 (Server Core installation)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV: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	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 for x64-based Systems	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0634						
Windows 10 Version 1607 for x64-based Systems	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based	4534310 Monthly Rollup	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7	Yes

CVE-2020-0634						
Systems Service Pack 1	4534314 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 8.1 for 32-bit systems	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based systems	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4534297 Monthly Rollup	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0634						
Windows Server 2008 for 32-bit Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 (Server Core installation)	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 Itanium-Based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0634						
Windows Server 2008 for x64-based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based Systems Service Pack 2 (Server Core installation)	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0634						
Service Pack 1						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based Systems Service Pack 1 (Server Core installation)	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534283 Monthly Rollup 4534288 Security	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0634						
	Only					
Windows Server 2012 (Server Core installation)	4534283 Monthly Rollup 4534288 Security Only	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 R2	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 R2 (Server Core installation)	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0634						
Windows 10 Version 1909 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0635 - Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0635 MITRE NVD	**CVE Title:** Windows Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Microsoft Windows when Windows fails to properly handle certain symbolic links. An attacker who successfully exploited this vulnerability could potentially set certain items to run at a higher level and thereby elevate permissions. 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 handles symbolic links. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0635						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0635						
Windows 10 Version 1803 for x64-based Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0635						
Windows 10 Version 1809 for x64-based Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0635						
Windows 10 Version 1709 for x64-based Systems	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 ARM64-based Systems	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 1903 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7	Yes

CVE-2020-0635						
ARM64-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 1903 (Server Core installation)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV: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	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 for x64-based Systems	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0635						
Windows 10 Version 1607 for x64-based Systems	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based	4534310 Monthly Rollup	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7	Yes

CVE-2020-0635						
Systems Service Pack 1	4534314 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 8.1 for 32-bit systems	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based systems	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4534297 Monthly Rollup	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0635						
Windows Server 2008 for 32-bit Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 (Server Core installation)	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 Itanium-Based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0635						
Windows Server 2008 for x64-based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based Systems Service Pack 2 (Server Core installation)	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0635						
Service Pack 1						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based Systems Service Pack 1 (Server Core installation)	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534283 Monthly Rollup 4534288 Security	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0635						
	Only					
Windows Server 2012 (Server Core installation)	4534283 Monthly Rollup 4534288 Security Only	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 R2	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 R2 (Server Core installation)	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0635						
Windows 10 Version 1909 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0636 - Windows Subsystem for Linux Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0636 MITRE NVD	**CVE Title:** Windows Subsystem for Linux Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way that the Windows Subsystem for Linux handles files. An attacker who successfully exploited the vulnerability could execute code with elevated privileges. To exploit the vulnerability, an attacker would first need code execution on a victim system. An attacker could then run a specially crafted application. The security update addresses the vulnerability by correcting how the Windows Subsystem for Linux handles files. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0636						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1903 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7	Yes

CVE-2020-0636						
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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0636						
Windows 10 Version 1909 for ARM64-based Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0637 - Remote Desktop Web Access Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-	**CVE Title:** Remote Desktop Web Access Information Disclosure Vulnerability **Description:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
0637 MITRE NVD	An information disclosure vulnerability exists when Remote Desktop Web Access improperly handles credential information. An attacker who successfully exploited this vulnerability could obtain legitimate users' credentials. To exploit this vulnerability, an attacker would need access to a vulnerable server with the Remote Desktop Web Access role. The security update addresses the vulnerability by correcting how Remote Desktop Web Access handles credential information. **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 sensitive information. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 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-2020-0637						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2019	4534273 Security Update	Important	Information Disclosure	4530715	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2019 (Server Core	4534273 Security Update	Important	Information Disclosure	4530715	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-0637						
installation)						
Windows Server 2016	4534271 Security Update	Important	Information Disclosure	4530689	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2016 (Server Core installation)	4534271 Security Update	Important	Information Disclosure	4530689	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/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	4534310 Monthly Rollup 4534314 Security Only	Important	Information Disclosure	4530734	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2020-0637						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4534310 Monthly Rollup 4534314 Security Only	Important	Information Disclosure	4530734	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4534283 Monthly Rollup 4534288 Security Only	Important	Information Disclosure	4530691	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2012	4534283 Monthly	Important	Information Disclosure	4530691	Base: 5.7 Temporal: 5.1 Vector:	Unknown

CVE-2020-0637						
(Server Core installation)	Rollup 4534288 Security Only				CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2012 R2	4534297 Monthly Rollup 4534309 Security Only	Important	Information Disclosure	4530702	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2012 R2 (Server Core installation)	4534297 Monthly Rollup 4534309 Security	Important	Information Disclosure	4530702	Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2020-0637						
	Only					

CVE-2020-0638 - Update Notification Manager Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0638 MITRE NVD	**CVE Title:** Update Notification Manager Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way the Update Notification Manager handles files. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how the Update Notification Manager handles files. **FAQ:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0638						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version	4534276 Security	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7	Unknown

CVE-2020-0638						
1709 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 32-bit Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 1903 for ARM64-based Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0638						
Windows 10 Version 1709 for ARM64-based Systems	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0638						
Windows 10 Version 1903 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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 x64-based Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 1903 for x64-based Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 2019	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0638						
Windows Server, version 1803 (Server Core Installation)	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 1903 (Server Core installation)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0638						
Windows Server, version 1909 (Server Core installation)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0639 - Windows Common Log File System Driver Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0639 MITRE NVD	**CVE Title:** Windows Common Log File System Driver Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could potentially read data that was not intended to be disclosed. Note that this vulnerability would not allow an attacker to execute code or to elevate their user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system. 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.	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 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 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0639						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Information Disclosure	4530717	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 1803 for x64-based Systems	4534293 Security Update	Important	Information Disclosure	4530717	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, version 1803 (Server Core Installation)	4534293 Security Update	Important	Information Disclosure	4530717	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 1803 for	4534293 Security	Important	Information Disclosure	4530717	Base: 5.5 Temporal: 5 Vector:	Unknown

CVE-2020-0639						
ARM64-based Systems	Update				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 32-bit Systems	4534273 Security Update	Important	Information Disclosure	4530715	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	4534273 Security Update	Important	Information Disclosure	4530715	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	4534273 Security Update	Important	Information Disclosure	4530715	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	4534273 Security Update	Important	Information Disclosure	4530715	Base: 5.5 Temporal: 5 Vector:	Unknown

CVE-2020-0639						
					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 (Server Core installation)	4534273 Security Update	Important	Information Disclosure	4530715	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 1709 for 32-bit Systems	4534276 Security Update	Important	Information Disclosure	4530714	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 1709 for x64-based Systems	4534276 Security Update	Important	Information Disclosure	4530714	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 1709 for ARM64-	4534276 Security Update	Important	Information Disclosure	4530714	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-2020-0639						
based Systems						
Windows 10 Version 1903 for 32-bit Systems	4528760 Security Update	Important	Information Disclosure	4530684	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	4528760 Security Update	Important	Information Disclosure	4530684	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	4528760 Security Update	Important	Information Disclosure	4530684	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	4528760 Security Update	Important	Information Disclosure	4530684	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-2020-0639						
Core installation)						
Windows 10 for 32-bit Systems	4534306 Security Update	Important	Information Disclosure	4530681	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 for x64-based Systems	4534306 Security Update	Important	Information Disclosure	4530681	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 32-bit Systems	4534271 Security Update	Important	Information Disclosure	4530689	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	4534271 Security Update	Important	Information Disclosure	4530689	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-2020-0639						
Windows Server 2016	4534271 Security Update	Important	Information Disclosure	4530689	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)	4534271 Security Update	Important	Information Disclosure	4530689	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	4534310 Monthly Rollup 4534314 Security Only	Important	Information Disclosure	4530734	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 7 for x64-based Systems	4534310 Monthly Rollup 4534314 Security	Important	Information Disclosure	4530734	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-2020-0639						
Service Pack 1	Only					
Windows 8.1 for 32-bit systems	4534297 Monthly Rollup 4534309 Security Only	Important	Information Disclosure	4530702	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 8.1 for x64-based systems	4534297 Monthly Rollup 4534309 Security Only	Important	Information Disclosure	4530702	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 RT 8.1	4534297 Monthly Rollup	Important	Information Disclosure	4530702	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	4534303 Monthly	Important	Information Disclosure	4530695	Base: 5.5 Temporal: 5	Yes

CVE-2020-0639						
2008 for 32-bit Systems Service Pack 2	Rollup 4534312 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 Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4534303 Monthly Rollup 4534312 Security Only	Important	Information Disclosure	4530695	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 2008 for Itanium-Based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Information Disclosure	4530695	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-2020-0639						
Windows Server 2008 for x64-based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Information Disclosure	4530695	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 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4534303 Monthly Rollup 4534312 Security Only	Important	Information Disclosure	4530695	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 2008 R2 for Itanium-Based Systems	4534310 Monthly Rollup 4534314 Security	Important	Information Disclosure	4530734	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-2020-0639						
Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Information Disclosure	4530734	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 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4534310 Monthly Rollup 4534314 Security Only	Important	Information Disclosure	4530734	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	4534283 Monthly Rollup 4534288	Important	Information Disclosure	4530691	Base: 5.5 Temporal: 5 Vector:	Unknown

CVE-2020-0639						
	Security Only				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 2012 (Server Core installation)	4534283 Monthly Rollup 4534288 Security Only	Important	Information Disclosure	4530691	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 R2	4534297 Monthly Rollup 4534309 Security Only	Important	Information Disclosure	4530702	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 R2 (Server Core installation)	4534297 Monthly Rollup 4534309 Security	Important	Information Disclosure	4530702	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-2020-0639						
	Only					
Windows 10 Version 1909 for 32-bit Systems	4528760 Security Update	Important	Information Disclosure	4530684	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	4528760 Security Update	Important	Information Disclosure	4530684	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	4528760 Security Update	Important	Information Disclosure	4530684	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	4528760 Security Update	Important	Information Disclosure	4530684	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-2020-0639						
Core installation)						

CVE-2020-0640 - Internet Explorer Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0640 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 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0640						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 10 on Windows Server 2012	4534283 Monthly Rollup 4534251 IE Cumulative	Moderate	Remote Code Execution	4530677	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 32-bit Systems Service Pack 2	4534251 IE Cumulative 4534303 Monthly Rollup	Moderate	Remote Code Execution	4530695	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-2020-0640						
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4534251 IE Cumulative 4534303 Monthly Rollup	Moderate	Remote Code Execution	4530695	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	4534293 Security Update	Critical	Remote Code Execution	4530717	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	4534293 Security	Critical	Remote Code Execution	4530717	Base: 7.5 Temporal: 6.7	Unknown

CVE-2020-0640						
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	4534293 Security Update	Critical	Remote Code Execution	4530717	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	4534273 Security Update	Critical	Remote Code Execution	4530715	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-2020-0640						
1809 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4534273 Security Update	Critical	Remote Code Execution	4530715	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	4534273 Security Update	Critical	Remote Code Execution	4530715	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-2020-0640						
Internet Explorer 11 on Windows Server 2019	4534273 Security Update	Moderate	Remote Code Execution	4530715	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 1709 for 32-bit Systems	4534276 Security Update	Critical	Remote Code Execution	4530714	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 1709 for x64-	4534276 Security Update	Critical	Remote Code Execution	4530714	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-2020-0640						
based Systems						
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems	4534276 Security Update	Critical	Remote Code Execution	4530714	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 1903 for 32-bit Systems	4528760 Security Update	Critical	Remote Code Execution	4530684	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-2020-0640						
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems	4528760 Security Update	Critical	Remote Code Execution	4530684	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	4528760 Security Update	Critical	Remote Code Execution	4530684	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	4534306 Security	Critical	Remote Code Execution	4530681	Base: 7.5 Temporal: 6.7	Unknown

CVE-2020-0640						
Windows 10 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 for x64-based Systems	4534306 Security Update	Critical	Remote Code Execution	4530681	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 32-bit Systems	4534271 Security Update	Critical	Remote Code Execution	4530689	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-2020-0640						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4534271 Security Update	Critical	Remote Code Execution	4530689	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	4534271 Security Update	Moderate	Remote Code Execution	4530689	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	4534251 IE Cumulative 4534310 Monthly Rollup	Critical	Remote Code Execution	4530734	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-2020-0640						
Service Pack 1						
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4534251 IE Cumulative 4534310 Monthly Rollup	Critical	Remote Code Execution	4530734	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 32-bit systems	4534251 IE Cumulative 4534297 Monthly Rollup	Critical	Remote Code Execution	4530702	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	4534251 IE Cumulative 4534297 Monthly	Critical	Remote Code Execution	4530702	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-2020-0640						
8.1 for x64-based systems	Rollup					
Internet Explorer 11 on Windows RT 8.1	4534297 Monthly Rollup	Critical	Remote Code Execution	4530702	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 2008 R2 for x64-based Systems Service Pack 1	4534251 IE Cumulative 4534310 Monthly Rollup	Moderate	Remote Code Execution	4530734	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	4534251 IE Cumulative	Moderate	Remote Code Execution	4530677	Base: 6.4 Temporal: 5.8	Yes

CVE-2020-0640						
Windows Server 2012					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 Server 2012 R2	4534251 IE Cumulative 4534297 Monthly Rollup	Moderate	Remote Code Execution	4530702	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	4528760 Security Update	Critical	Remote Code Execution	4530684	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	4528760 Security Update	Critical	Remote Code Execution	4530684	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-2020-0640						
Version 1909 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1909 for ARM64-based Systems	4528760 Security Update	Critical	Remote Code Execution	4530684	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-2020-0641 - Microsoft Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0641 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. 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 01/14/2020 08:00:00	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-2020-0641						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0641						
Windows Server, version 1803 (Server Core Installation)	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0641						
Windows 10 Version 1809 for ARM64-based Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0641						
Windows 10 Version 1709 for ARM64-based Systems	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 1903 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0641						
Windows Server, version 1903 (Server Core installation)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV: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	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 for x64-based Systems	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0641						
Windows Server 2016	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based systems	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0641						
Windows RT 8.1	4534297 Monthly Rollup	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534283 Monthly Rollup 4534288 Security Only	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 (Server Core installation)	4534283 Monthly Rollup 4534288 Security Only	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 R2	4534297 Monthly Rollup 4534309 Security	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0641						
	Only					
Windows Server 2012 R2 (Server Core installation)	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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-	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0641						
based Systems						
Windows Server, version 1909 (Server Core installation)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0642 - Win32k Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0642 MITRE NVD	**CVE Title:** Win32k Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows when the Win32k component 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.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 Win32k handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0642						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0642						
Windows 10 Version 1803 for ARM64-based Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0642						
Windows Server 2019	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 ARM64-based Systems	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0642						
Windows 10 Version 1903 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0642						
Windows 10 for 32-bit Systems	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 for x64-based Systems	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0642						
Windows Server 2016 (Server Core installation)	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit systems	4534297 Monthly Rollup 4534309 Security	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0642						
	Only					
Windows 8.1 for x64-based systems	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4534297 Monthly Rollup	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534303 Monthly Rollup	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7	Yes

CVE-2020-0642						
Systems Service Pack 2 (Server Core installation)	4534312 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 2008 for Itanium-Based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based	4534303 Monthly Rollup 4534312	Important	Elevation of Privilege	4530695	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0642						
Systems Service Pack 2 (Server Core installation)	Security Only					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-	4534310 Monthly Rollup	Important	Elevation of Privilege	4530734	Base: 7.8 Temporal: 7	Yes

CVE-2020-0642						
based Systems Service Pack 1 (Server Core installation)	4534314 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	4534283 Monthly Rollup 4534288 Security Only	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 (Server Core installation)	4534283 Monthly Rollup 4534288 Security Only	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 R2	4534297 Monthly Rollup	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7	Unknown

CVE-2020-0642						
	4534309 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 R2 (Server Core installation)	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7	Yes

CVE-2020-0642						
ARM64-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 1909 (Server Core installation)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0643 - Windows GDI+ Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0643 MITRE NVD	**CVE Title:** Windows GDI+ Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface Plus (GDI+) handles objects in memory, allowing an attacker to retrieve information from a targeted system. By itself, the information disclosure does not allow	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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. **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 01/14/2020 08:00:00 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-2020-0643						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Information Disclosure	4530717	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 1803 for x64-based Systems	4534293 Security Update	Important	Information Disclosure	4530717	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-2020-0643						
Windows Server, version 1803 (Server Core Installation)	4534293 Security Update	Important	Information Disclosure	4530717	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 1803 for ARM64-based Systems	4534293 Security Update	Important	Information Disclosure	4530717	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 32-bit Systems	4534273 Security Update	Important	Information Disclosure	4530715	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	4534273 Security Update	Important	Information Disclosure	4530715	Base: 5.5 Temporal: 5 Vector:	Unknown

CVE-2020-0643						
x64-based Systems					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 ARM64-based Systems	4534273 Security Update	Important	Information Disclosure	4530715	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	4534273 Security Update	Important	Information Disclosure	4530715	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)	4534273 Security Update	Important	Information Disclosure	4530715	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 1709 for	4534276 Security Update	Important	Information Disclosure	4530714	Base: 5.5 Temporal: 5 Vector:	Unknown

CVE-2020-0643						
32-bit Systems					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	4534276 Security Update	Important	Information Disclosure	4530714	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 1709 for ARM64-based Systems	4534276 Security Update	Important	Information Disclosure	4530714	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 1903 for 32-bit Systems	4528760 Security Update	Important	Information Disclosure	4530684	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	4528760 Security Update	Important	Information Disclosure	4530684	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-2020-0643						
Windows 10 Version 1903 for ARM64-based Systems	4528760 Security Update	Important	Information Disclosure	4530684	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)	4528760 Security Update	Important	Information Disclosure	4530684	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	4534306 Security Update	Important	Information Disclosure	4530681	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 for x64-based Systems	4534306 Security Update	Important	Information Disclosure	4530681	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-2020-0643						
Windows 10 Version 1607 for 32-bit Systems	4534271 Security Update	Important	Information Disclosure	4530689	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	4534271 Security Update	Important	Information Disclosure	4530689	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	4534271 Security Update	Important	Information Disclosure	4530689	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)	4534271 Security Update	Important	Information Disclosure	4530689	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	4534310 Monthly	Important	Information Disclosure	4530734	Base: 5.5 Temporal: 5	Yes

CVE-2020-0643						
Systems Service Pack 1	Rollup 4534314 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 7 for x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Information Disclosure	4530734	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 32-bit systems	4534297 Monthly Rollup 4534309 Security Only	Important	Information Disclosure	4530702	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 8.1 for x64-based systems	4534297 Monthly Rollup 4534309	Important	Information Disclosure	4530702	Base: 5.5 Temporal: 5 Vector:	Unknown

CVE-2020-0643						
	Security Only				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 RT 8.1	4534297 Monthly Rollup	Important	Information Disclosure	4530702	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	4534303 Monthly Rollup 4534312 Security Only	Important	Information Disclosure	4530695	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 2008 for 32-bit Systems Service Pack 2 (Server	4534303 Monthly Rollup 4534312 Security Only	Important	Information Disclosure	4530695	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-2020-0643						
Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Information Disclosure	4530695	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 2008 for x64-based Systems Service Pack 2	4534303 Monthly Rollup 4534312 Security Only	Important	Information Disclosure	4530695	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 2008 for x64-based Systems Service	4534303 Monthly Rollup 4534312 Security	Important	Information Disclosure	4530695	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-2020-0643						
Pack 2 (Server Core installation)	Only					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Information Disclosure	4530734	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 2008 R2 for x64-based Systems Service Pack 1	4534310 Monthly Rollup 4534314 Security Only	Important	Information Disclosure	4530734	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 2008 R2 for x64-based	4534310 Monthly Rollup 4534314	Important	Information Disclosure	4530734	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2020-0643						
Systems Service Pack 1 (Server Core installation)	Security Only				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 2012	4534283 Monthly Rollup 4534288 Security Only	Important	Information Disclosure	4530691	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 (Server Core installation)	4534283 Monthly Rollup 4534288 Security Only	Important	Information Disclosure	4530691	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 R2	4534297 Monthly Rollup	Important	Information Disclosure	4530702	Base: 5.5 Temporal: 5 Vector:	Unknown

CVE-2020-0643						
	4534309 Security Only				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 2012 R2 (Server Core installation)	4534297 Monthly Rollup 4534309 Security Only	Important	Information Disclosure	4530702	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	4528760 Security Update	Important	Information Disclosure	4530684	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	4528760 Security Update	Important	Information Disclosure	4530684	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	4528760 Security	Important	Information Disclosure	4530684	Base: 5.5 Temporal: 5	Yes

CVE-2020-0643						
1909 for ARM64-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 1909 (Server Core installation)	4528760 Security Update	Important	Information Disclosure	4530684	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-2020-0644 - Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0644	**CVE Title:** Windows Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft Windows implements predictable memory section names. An attacker who successfully exploited this	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	vulnerability could run arbitrary code as system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit the vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application designed to elevate privileges. The update addresses the vulnerability by correcting how Windows assigns memory to specific processes. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0644						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0644						
Windows 10 Version 1803 for ARM64-based Systems	4534293 Security Update	Important	Elevation of Privilege	4530717	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0644						
Windows Server 2019	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4534273 Security Update	Important	Elevation of Privilege	4530715	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 ARM64-based Systems	4534276 Security Update	Important	Elevation of Privilege	4530714	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0644						
Windows 10 Version 1903 for 32-bit Systems	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0644						
Windows 10 for 32-bit Systems	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 for x64-based Systems	4534306 Security Update	Important	Elevation of Privilege	4530681	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 32-bit Systems	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0644						
Windows Server 2016 (Server Core installation)	4534271 Security Update	Important	Elevation of Privilege	4530689	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 x64-based systems	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4534297 Monthly Rollup	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0644						
Windows Server 2012	4534283 Monthly Rollup 4534288 Security Only	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 (Server Core installation)	4534283 Monthly Rollup 4534288 Security Only	Important	Elevation of Privilege	4530691	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 R2	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2020-0644						
Windows Server 2012 R2 (Server Core installation)	4534297 Monthly Rollup 4534309 Security Only	Important	Elevation of Privilege	4530702	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0644						
Windows Server, version 1909 (Server Core installation)	4528760 Security Update	Important	Elevation of Privilege	4530684	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2020-0646 - .NET Framework Remote Code Execution Injection Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0646 MITRE NVD	**CVE Title:** .NET Framework Remote Code Execution Injection Vulnerability **Description:** A remote code execution vulnerability exists when the Microsoft .NET Framework fails to validate input properly. An attacker who successfully exploited this 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. Users whose	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. To exploit the vulnerability, an attacker would need to pass specific input to an application utilizing susceptible .Net methods. The security update addresses the vulnerability by correcting how the Microsoft .NET Framework validates input. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0646						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0646						
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	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	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	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	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	4535104 Monthly Rollup	Critical	Remote Code Execution	4524743; 4533097	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	4535102 Monthly Rollup 4534976	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A	Maybe

CVE-2020-0646						
	Security Only				Vector: N/A	
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)	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	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	4535103 Monthly Rollup 4534977 Security Only	Critical	Remote Code Execution	4524742; 4533096	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)	4535103 Monthly Rollup 4534977 Security	Critical	Remote Code Execution	4524742; 4533096	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0646						
	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	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	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 (Server Core installation)	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for 32-bit Systems	4534271 Security Update	Critical	Remote Code Execution	4530689	Base: N/A Temporal: N/A Vector: N/A	Unknown

CVE-2020-0646						
Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for 32-bit Systems	4532936 Security Update	Critical	Remote Code Execution	4530689	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for x64-based Systems	4532936 Security Update	Critical	Remote Code Execution	4530689	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server, version 1803 (Server Core Installation)	4532936 Security Update	Critical	Remote Code Execution	4530689	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for 32-bit Systems	4532935 Security Update	Critical	Remote Code Execution	4530689	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for x64-based Systems	4532935 Security	Critical	Remote Code Execution	4530689	Base: N/A Temporal: N/A	Maybe

CVE-2020-0646						
	Update				Vector: N/A	
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for 32-bit Systems	4532933 Security Update	Critical	Remote Code Execution	4530689	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for x64-based Systems	4532933 Security Update	Critical	Remote Code Execution	4530689	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2016	4532933 Security Update	Critical	Remote Code Execution	4530689	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2016 (Server Core installation)	4532933 Security Update	Critical	Remote Code Execution	4530689	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0646						
Microsoft .NET Framework 4.8 on Windows 7 for 32-bit Systems Service Pack 1	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 8.1 for 32-bit systems	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0646						
Microsoft .NET Framework 4.8 on Windows 8.1 for x64-based systems	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows RT 8.1	4535104 Monthly Rollup	Critical	Remote Code Execution	4524743; 4533097	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	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)	4535102 Monthly Rollup 4534976	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A	Maybe

CVE-2020-0646						
	Security Only				Vector: N/A	
Microsoft .NET Framework 4.8 on Windows Server 2012	4535103 Monthly Rollup 4534977 Security Only	Critical	Remote Code Execution	4524742; 4533096	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 (Server Core installation)	4535103 Monthly Rollup 4534977 Security Only	Critical	Remote Code Execution	4524742; 4533096	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 R2	4535104 Monthly Rollup 4534978 Security	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0646						
	Only					
Microsoft .NET Framework 4.8 on Windows Server 2012 R2 (Server Core installation)	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1809 for 32-bit Systems	4535101 Security Update	Critical	Remote Code Execution	4524743; 4533097	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	4535101 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server 2019	4535101 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A	Maybe

CVE-2020-0646						
					Vector: N/A	
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server 2019 (Server Core installation)	4535101 Security Update	Critical	Remote Code Execution	4524743; 4533097	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	4532938 Security Update	Critical	Remote Code Execution	4524743; 4533097	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	4532938 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server, version 1903 (Server Core installation)	4532938 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0646						
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1809 for 32-bit Systems	4535101 Security Update	Critical	Remote Code Execution	4524743; 4533097	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	4535101 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server 2019	4535101 Security Update	Critical	Remote Code Execution	4524743; 4533097	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)	4535101 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2	4535105 Monthly Rollup	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A	Maybe

CVE-2020-0646						
	4534979 Security Only				Vector: N/A	
Microsoft .NET Framework 4.6 on Windows Server 2008 for x64-based Systems Service Pack 2	4535105 Monthly Rollup 4534979 Security Only	Critical	Remote Code Execution	4524743; 4533097	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	4535105 Monthly Rollup 4534979 Security Only	Critical	Remote Code Execution	4524743; 4533097	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	4535105 Monthly Rollup 4534979 Security	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0646						
	Only					
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2	4535105 Monthly Rollup 4534979 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for 32-bit Systems	4534271 Security Update	Critical	Remote Code Execution	4530689	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0646						
Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012	4535103 Monthly Rollup 4534977 Security Only	Critical	Remote Code Execution	4524742; 4533096	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation)	4535103 Monthly Rollup 4534977 Security Only	Critical	Remote Code Execution	4524742; 4533096	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0646						
Microsoft .NET Framework 3.5 on Windows Server 2012 R2	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation)	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0646						
Microsoft .NET Framework 3.5.1 on Windows 7 for x64-based Systems Service Pack 1	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0646						
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0646						
Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows RT 8.1	4535104 Monthly Rollup	Critical	Remote Code Execution	4524743; 4533097	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	4535105 Monthly Rollup 4534979	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A	Maybe

CVE-2020-0646						
	Security Only				Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for x64-based Systems Service Pack 2	4535105 Monthly Rollup 4534979 Security Only	Critical	Remote Code Execution	4524743; 4533097	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	4535102 Monthly Rollup 4534976 Security Only	Critical	Remote Code Execution	4524741; 4533095	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)	4535102 Monthly Rollup 4534976 Security	Critical	Remote Code Execution	4524741; 4533095	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0646						
	Only					
Microsoft .NET Framework 4.5.2 on Windows Server 2012	4535103 Monthly Rollup 4534977 Security Only	Critical	Remote Code Execution	4524742; 4533096	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation)	4535103 Monthly Rollup 4534977 Security Only	Critical	Remote Code Execution	4524742; 4533096	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0646						
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation)	4535104 Monthly Rollup 4534978 Security Only	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1909 for 32-bit Systems	4532938 Security Update	Critical	Remote Code Execution	4524743; 4533097	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)	4532938 Security Update	Critical	Remote Code Execution	4524743; 4533097	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	4532938 Security Update	Critical	Remote Code Execution	4524743; 4533097	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0646						
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server, version 1803 (Server Core Installation)	4534293 Security Update	Critical	Remote Code Execution	4530717	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 for 32-bit Systems	4534306 Security Update	Critical	Remote Code Execution	4530681	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1803 for 32-bit Systems	4534293 Security Update	Critical	Remote Code Execution	4530717	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1803 for x64-based Systems	4534293 Security Update	Critical	Remote Code Execution	4530717	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 3.5 AND 4.7.1/4.7.2 on Windows 10 Version 1709 for x64-based Systems	4534276 Security	Critical	Remote Code Execution	4530714	Base: N/A Temporal: N/A	Unknown

CVE-2020-0646						
	Update				Vector: N/A	
Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016 (Server Core installation)	4534271 Security Update	Critical	Remote Code Execution	4530689	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 for x64-based Systems	4534306 Security Update	Critical	Remote Code Execution	4530681	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 32-bit Systems	4534271 Security Update	Critical	Remote Code Execution	4530689	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 3.5 AND 4.7.1/4.7.2 on Windows 10 Version 1709 for 32-bit Systems	4534276 Security Update	Critical	Remote Code Execution	4530714	Base: N/A Temporal: N/A Vector: N/A	Unknown

CVE-2020-0646						
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	4534271 Security Update	Critical	Remote Code Execution	4530689	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	4534271 Security Update	Critical	Remote Code Execution	4530689	Base: N/A Temporal: N/A Vector: N/A	Unknown

CVE-2020-0647 - Microsoft Office Online Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0647 MITRE NVD	**CVE Title:** Microsoft Office Online Spoofing Vulnerability **Description:** A spoofing vulnerability exists when Office Online does not validate origin in cross-origin communications correctly. An attacker could exploit the vulnerability by sending a specially crafted request to an affected site.	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The attacker who successfully exploited the vulnerability could then perform cross-origin attacks on affected systems. These attacks could allow the attacker to read content that the attacker is not authorized to read, and use the victim's identity to take actions on the site on behalf of the victim. The victim needs to be authenticated for an attacker to compromise the victim. The security update addresses the vulnerability by ensuring that Office Online properly validates origins. **FAQ:** **Is the Preview Pane an attack vector for this vulnerability?** No, the Preview Pane is not an attack vector. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 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-2020-0647						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Office Online Server	4484223 Security Update	Important	Spoofing	4484141	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0650 - Microsoft Excel Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0650 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. 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	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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:** **Is the Preview Pane an attack vector for this vulnerability?** No, the Preview Pane is not an attack vector. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0650						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2019 for 32-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 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
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	No

CVE-2020-0650						
Office 365 ProPlus for 64-bit Systems	Click to Run Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Excel 2016 (32-bit edition)	4484217 Security Update	Important	Remote Code Execution	4484179	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 (64-bit edition)	4484217 Security Update	Important	Remote Code Execution	4484179	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 for Mac	Release Notes Security Update	Important	Remote Code Execution	4484179	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Excel 2010 Service Pack 2 (32-bit editions)	4484243 Security Update	Important	Remote Code Execution	4484196	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2010 Service Pack 2 (64-bit editions)	4484243 Security Update	Important	Remote Code Execution	4484196	Base: N/A Temporal:	Maybe

CVE-2020-0650						
					N/A Vector: N/A	
Microsoft Excel 2013 RT Service Pack 1	4484234 Security Update	Important	Remote Code Execution	4484190	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (32-bit editions)	4484234 Security Update	Important	Remote Code Execution	4484190	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (64-bit editions)	4484234 Security Update	Important	Remote Code Execution	4484190	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0651 - Microsoft Excel Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0651 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. 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	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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:** **Is the Preview Pane an attack vector for this vulnerability?** No, the Preview Pane is not an attack vector. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0651						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2019 for 32-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 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
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	No

CVE-2020-0651						
Office 365 ProPlus for 64-bit Systems	Click to Run Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Excel 2016 (32-bit edition)	4484217 Security Update	Important	Remote Code Execution	4484179	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 (64-bit edition)	4484217 Security Update	Important	Remote Code Execution	4484179	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 for Mac	Release Notes Security Update	Important	Remote Code Execution	4484179	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Excel 2010 Service Pack 2 (32-bit editions)	4484243 Security Update	Important	Remote Code Execution	4484196	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2010 Service Pack 2 (64-bit editions)	4484243 Security Update	Important	Remote Code Execution	4484196	Base: N/A Temporal:	Maybe

CVE-2020-0651						
					N/A Vector: N/A	
Microsoft Excel 2013 RT Service Pack 1	4484234 Security Update	Important	Remote Code Execution	4484190	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (32-bit editions)	4484234 Security Update	Important	Remote Code Execution	4484190	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (64-bit editions)	4484234 Security Update	Important	Remote Code Execution	4484190	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0652 - Microsoft Office Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0652 MITRE NVD	**CVE Title:** Microsoft Office Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office 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. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office software. 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) that contains 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	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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. Note that the Preview Pane is not an attack vector for this vulnerability. The security update addresses the vulnerability by correcting how Office handles objects in memory. **FAQ:** **Is the Preview Pane an attack vector for this vulnerability?** No, the Preview Pane is not an attack vector. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0652						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2019 for 32-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 64-bit editions	Click to Run Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	No
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	No
Office 365 ProPlus for 64-bit Systems	Click to Run Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	No

CVE-2020-0652						
Microsoft Office 2016 (32-bit edition)	4484221 Security Update	Important	Remote Code Execution	4484182	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	4484221 Security Update	Important	Remote Code Execution	4484182	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4484236 Security Update	Important	Remote Code Execution	4484192	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4484236 Security Update	Important	Remote Code Execution	4484192	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 RT Service Pack 1	4484227 Security Update	Important	Remote Code Execution	4484184	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4484227 Security Update	Important	Remote Code Execution	4484184	Base: N/A Temporal:	Maybe

CVE-2020-0652						
					N/A Vector: N/A	
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4484227 Security Update	Important	Remote Code Execution	4484184	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0653 - Microsoft Excel Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0653 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	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. 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:** **Is the Preview Pane an attack vector for this vulnerability?** No, the Preview Pane is not an attack vector. **Mitigations:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0653						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	No

CVE-2020-0653						
Office 365 ProPlus for 64-bit Systems	Click to Run Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	No

CVE-2020-0654 - Microsoft OneDrive for Android Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0654 MITRE NVD	**CVE Title:** Microsoft OneDrive for Android Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists in Microsoft OneDrive App for Android. This could allow an attacker to bypass the passcode or fingerprint requirements of the App. The security update addresses the vulnerability by correcting the way Microsoft OneDrive App for Android handles sharing links.	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: **How do I get the update for OneDrive for Android?** 1. Tap the **Google Play** icon on your home screen. 2. Swipe in from the left edge of the screen. 3. Tap **My apps & games**. 4. Tap the Update box next to the **OneDrive app**. **Is there a direct link on the web?** Yes: https://play.google.com/store/apps/details?id=com.microsoft.skydrive&hl=en_US **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0654						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
One Drive for Android	Release Notes Security Update	Important	Security Feature Bypass		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2020-0656 - Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2020-0656	**CVE Title:** Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability **Description:**	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	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. **FAQ:** None **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 01/14/2020 08:00:00 Information published.		

Affected Software

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

CVE-2020-0656						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Dynamics 365 Field Service (on-premises) v7 series	Relelase Notes Security Update	Important	Spoofing		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 Information Technology Co. Ltd., the company has operations in the Americas, Europe, the Middle East and Asia Pacific.