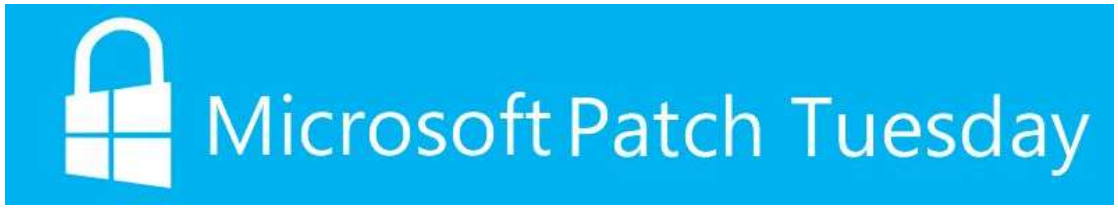
Microsoft's December 2019 Security Update Fixes 38 Security Vulnerabilities



Overview

Microsoft released 2019 December security update on Tuesday that fixes 38 security issues ranging from simple spoofing attacks to remote code execution in various products, including End of Life Software, Microsoft Graphics Component, Microsoft Office, Microsoft Scripting Engine, Microsoft Windows, None, Open Source Software, Servicing Stack Updates, Skype for Business, SQL Server, Visual Studio, Windows Hyper-V, Windows Kernel, Windows Media Player, and Windows OLE.
Of the vulnerabilities fixed by Microsoft's update of this month, seven are critical, which are located in Hyper-V, Windows font library, and Visual Studio. In addition, some of those vulnerabilities are important ones.

Critical Vulnerabilities

The following are seven critical vulnerabilities covered in this update.

CVE-2019-1468

This is a remote code execution vulnerability in the Windows font library, which stems from the library's inability to properly handle certain embedded fonts. Via a specially crafted malicious embedded font on a web page, an attacker could exploit this vulnerability to persuade users to visit the web page or open a specially crafted font file on their computer to execute code remotely.

For more details about the vulnerability and related updates, please refer to Microsoft's official security bulletins:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1468

CVE-2019-1471

This is a remote code execution vulnerability in the Hyper-V hypervisor. Sometimes, Hyper-V may fail to properly validate input by authenticated users on the guest operating system. An attacker could exploit this vulnerability by running a specially designed application on the guest OS, which would allow the Hyper-V host OS to execute arbitrary code on the host operating system.

For more details about the vulnerability and related updates, please refer to Microsoft's official security bulletins:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1471

Visual Studio

There are several key vulnerabilities in Git for Visual Studio (CVE-2019-1349, CVE-2019-1350, CVE-2019-1352, CVE-2019-1354, CVE-2019-1387).

Git for Visual Studio has an input validation issue which could lead to a remote code execution vulnerability. An attacker who successfully exploits 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.
To exploit this vulnerability, an attacker first needs to convince users to clone a malicious repository.

For more details about the vulnerability and related updates, please refer to Microsoft's official security bulletins:

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1349
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1350
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1352
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1354
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1387

Important Vulnerabilities

In addition to two critical vulnerabilities, this update also covers multiple important vulnerabilities, three of which require special attention.

CVE-2019-1458

This is a privilege elevation vulnerability in the Windows Win32k component. An attacker could exploit this vulnerability by logging into the system and then running a specially designed application, thus taking full control of the system and executing arbitrary code in kernel mode. Microsoft reports that this vulnerability has been widely exploited in the wild.
For more details about the vulnerability and related updates, please refer to Microsoft's official security bulletins:

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1458

CVE-2019-1469

This is an information disclosure vulnerability in Windows which is derived from the fact that the win32k component sometimes cannot provide kernel information. An attacker could exploit this vulnerability to obtain uninitialized memory and kernel memory and then use it for other attacks.
For more details about the vulnerability and related updates, please refer to Microsoft's official security bulletins:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1469

CVE-2019-1485

This is a remote code execution vulnerability in the VBscript engine. An attacker could exploit this vulnerability to corrupt the memory of an affected system, resulting in arbitrary code execution in the context of the current user. To trigger this vulnerability, users must visit a specially designed malicious website in an Internet Explorer browser. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the Internet Explorer rendering engine, and then convince the user to open the file.
For more details about the vulnerability and related updates, please refer to Microsoft's official security bulletins:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1485

Remediation

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

Product	CVE ID	CVE Title	Severity Level
End of Life Software	CVE-2019-1489	Remote Desktop Protocol Information Disclosure Vulnerability	Important
Microsoft Graphics Component	CVE-2019-1465	Windows GDI Information Disclosure Vulnerability	Important
Microsoft Graphics Component	CVE-2019-1466	Windows GDI Information Disclosure Vulnerability	Important
Microsoft Graphics Component	CVE-2019-1467	Windows GDI Information Disclosure Vulnerability	Important
Microsoft Graphics Component	CVE-2019-1468	Win32k Graphics Remote code execution vulnerability	Critical

Microsoft Office	CVE-2019-1400	Microsoft Access Information Disclosure Vulnerability	Important
Microsoft Office	CVE-2019-1461	Microsoft Word Denial of service vulnerability	Important
Microsoft Office	CVE-2019-1462	Microsoft PowerPoint Remote code execution vulnerability	Important
Microsoft Office	CVE-2019-1463	Microsoft Access Information Disclosure Vulnerability	Important
Microsoft Office	CVE-2019-1464	Microsoft Excel Information Disclosure Vulnerability	Important
Microsoft Scripting Engine	CVE-2019-1485	VBScript Remote code execution vulnerability	Important
Microsoft Windows	CVE-2019-1453	Windows Remote Desktop Protocol (RDP) Denial of service vulnerability	Important

Microsoft Windows	CVE-2019-1474	Windows Kernel Information Disclosure Vulnerability	Important
Microsoft Windows	CVE-2019-1483	Windows Elevation of Privilege Vulnerability	Important
Microsoft Windows	CVE-2019-1488	Microsoft Defender Security Function Bypass Vulnerability	Important
Microsoft Windows	CVE-2019-1476	Windows Elevation of Privilege Vulnerability	Important
Microsoft Windows	CVE-2019-1477	Windows Printer Service Elevation of Privilege Vulnerability	Important
Microsoft Windows	CVE-2019-1478	Windows COM Server Elevation of Privilege Vulnerability	Important
None	ADV190026	Microsoft Guidance for cleaning up orphaned keys generated on vulnerable TPMs and used for Windows Hello for Business	

Open Source Software	CVE-2019-1487	Microsoft Authentication Library for Android Information Disclosure Vulnerability	Important
Servicing Stack Updates	ADV990001	Latest Servicing Stack Updates	Critical
Skype for Business	CVE-2019-1490	Skype for Business Server Fraud	Important
SQL Server	CVE-2019-1332	Microsoft SQL Server Reporting Services XSS Vulnerability	Important
Visual Studio	CVE-2019-1349	Git for Visual Studio Remote code execution vulnerability	Critical
Visual Studio	CVE-2019-1350	Git for Visual Studio Remote code execution vulnerability	Critical
Visual Studio	CVE-2019-1351	Git for Visual Studio Tampering Vulnerability	Moderate
Visual Studio	CVE-2019-1352	Git for Visual Studio Remote code execution vulnerability	Critical

Visual Studio	CVE-2019-1354	Git for Visual Studio Remote code execution vulnerability	Critical
Visual Studio	CVE-2019-1387	Git for Visual Studio Remote code execution vulnerability	Critical
Visual Studio	CVE-2019-1486	Visual Studio Live Share Fraud	Important
Windows Hyper-V	CVE-2019-1470	Windows Hyper-V Information Disclosure Vulnerability	Important
Windows Hyper-V	CVE-2019-1471	Windows Hyper-V Remote code execution vulnerability	Critical
Windows Kernel	CVE-2019-1472	Windows Kernel Information Disclosure Vulnerability	Important
Windows Kernel	CVE-2019-1458	Win32k Elevation of Privilege Vulnerability	Important
Windows Kernel	CVE-2019-1469	Win32k Information Disclosure Vulnerability	Important

Windows Media Player	CVE-2019-1480	Windows Media Player Information Disclosure Vulnerability	Important
Windows Media Player	CVE-2019-1481	Windows Media Player Information Disclosure Vulnerability	Important
Windows OLE	CVE-2019-1484	Windows OLE Remote code execution vulnerability	Important

Recommended Mitigation Measures

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

Appendix

ADV190026 - Microsoft Guidance for cleaning up orphaned keys generated on vulnerable TPMs and used for Windows Hello for Business

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV190026 MITRE NVD	**CVE Title:** Microsoft Guidance for cleaning up orphaned keys generated on vulnerable TPMs and used for Windows Hello for Business **Description:** Microsoft is aware of an issue in Windows Hello for Business (WHfB) with public keys that persist after a device is removed from Active Directory, if the AD exists. After a user sets up Windows Hello for Business (WHfB), the WHfB public key is written to the on-premises Active Directory. The WHfB keys are tied to a user and a device that has been added to Azure AD, and if the device is removed, the corresponding WHfB key is considered orphaned. However, these orphaned keys are not deleted even when the device it was created on is no longer present. Any authentication to Azure AD using such an orphaned WHfB key will be rejected. However, some of these orphaned keys could lead to the following security issue in Active Directory 2016 or 2019, in either hybrid or on-premises environments.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	An authenticated attacker could obtain orphaned keys created on TPMs that were affected by CVE-2017-15361 (ROCA), discussed in Microsoft Security Advisory ADV170012 to compute their WHfB private key from the orphaned public keys. The attacker could then impersonate the user by using the stolen private key to authenticate as the user within the domain using Public Key Cryptography for Initial Authentication (PKINIT). This attack is possible even if firmware and software updates have been applied to TPMs that were affected by CVE-2017-15361 because the corresponding public keys might still exist in Active Directory. This advisory provides guidance for cleaning up any orphaned public keys that were generated with an unpatched TPM (before firmware updates discussed in ADV170012 were applied). Follow this guidance to identify and remove orphaned WHfB keys. This particular issue with orphaned public keys can be present when WHfB is set up in the following configurations: • WHfB is deployed on Active Directory 2016 or 2019, either in hybrid mode or on-premises only. • Currently have or have had in the past, WHfB keys generated on TPMs that were affected by CVE-2017-15361.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Important: Azure Active Directory (Azure AD) and Active Directory Federation Services (AD FS) are not affected by this issue. However, we strongly recommend that you follow the **Recommended Actions** section of ADV170012, and apply any firmware updates supplied by your TPM OEM, to avoid any exposure to Azure AD and AD FS. See Step #4 of the **Recommended Actions** for a list of OEMs and links to information for their updates. **FAQ:** **1. What systems are at risk?** Individual machines or servers are not affected by this WHfB issue. Affected environments are defined in the **Mitigations** section of this advisory. **2. Has this issue been publicly disclosed?** Yes, this issue has been disclosed. **3. Have there been any active attacks detected?** No. When this security advisory was issued, Microsoft had not received any information to indicate that this issue had been publicly used to attack customers. **4. How do I know if my TPMs are affected by CVE-2017-15361? How do I fix them?**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Please refer to Microsoft Security Advisory ADV170012 for more details on CVE-2017-15361. You must follow the guidance in ADV170012 and update your TPMs before applying the mitigations for identifying and removing the orphaned public keys. **5. I have updated all of my TPMs that were affected by CVE-2017-15361 with firmware provided by the OEM. Are my systems still affected?** Yes. Orphaned WHFB keys previously generated from those TPMs could still be stored in Active Directory. **6. My TPMs are not affected by CVE-2017-15361, but I do not enforce a policy to use TPMs for WHfB. Am I still affected?** In the absence of a hardware-required policy, WHFB will prefer using the TPM for storing the private key. If you do not have any TPMs that are affected by CVE-2017-15361, then you are not impacted. However, we recommend removing any orphaned keys in your directory by following the steps discussed in the **Mitigations** section of this advisory. **7. I am running pre-2016 versions of Active Directory. Do I also need to remove these orphaned keys?** While you are not affected by this WHFB issue, we strongly recommend removing these orphaned keys as a security hygiene measure.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	8. I regularly audit and clean up stale devices in my environment. How did I end up with orphaned keys? When a user provisions a WHFB credential, the public key is stored in the msDS-KeyCredentialLink attribute of the user object in Azure AD and on-premises Active Directory. If the device that was used to create the key is removed from Azure AD and Active Directory, the WHFB public key created for the user on that device is not automatically removed from the user object and it becomes an orphaned key. **9. I have deployed WHFB certificate trust in my environment and use certificates for authentication. Am I affected? Do I need to remove orphaned keys?** Yes. You are still affected by this issue if you have deployed certificate trust and have 2016 or 2019 DCs in your environment. These DC versions still support key-based authentication even if you have deployed end user certificates for authentication. **Mitigations:** **Workarounds:** None **Revision:** 1.0 12/03/2019 08:00:00		

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

Affected Software

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

ADV190026						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
None Available					Base: N/A Temporal: N/A Vector: N/A	

ADV990001 - Latest Servicing Stack Updates

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV990001 MITRE NVD	**CVE Title:** Latest Servicing Stack Updates **Description:** This is a list of the latest servicing stack updates for each operating system. This list will be updated whenever a new servicing stack update is released. It is important to install the latest servicing stack update. **FAQ:** **1. Why are all of the Servicing Stack Updates (SSU) critical updates?** The SSUs are classified as Critical updates. This does not indicate that there is a critical vulnerability being addressed in the update. **2. When was the most recent SSU released for each version of Microsoft Windows?** Please refer to the following table for the most recent SSU release. We will update the entries any time a new SSU is released: **Product** **SSU Package** **Date Released** Windows Server 2008 4531787 December 2019	Critical	Defense in Depth

CVE ID	Vulnerability Description			Maximum Severity Rating	Vulnerability Impact
	Windows 7/Server 2008 R2	4531786	December 2019		
	Windows Server 2012	4532920	December 2019		
	Windows 8.1/Server 2012 R2	4524445	November 2019		
	Windows 10	4523200	November 2019		
	Windows 10 Version 1607/Server 2016	4520724	November 2019		
	Windows 10 Version 1703	4521859	October 2019		
	Windows 10 1709	4523202	November 2019		
	Windows 10 1803/Windows Server, version 1803	4523203	November 2019		
	Windows 10 1809/Server 2019	4523204	November 2019		
	Windows 10 1903/Windows Server, version 1903	4524569	November 2019		
	3. Where can I find more information about the Servicing Stack Updates? You can find more information by following these links: • Servicing Stack Updates • Windows 7 servicing stack updates **Mitigations:** None				

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.2 12/03/2018 08:00:00 FAQs have been added to further explain Security Stack Updates. The FAQs include a table that indicates the most recent SSU release for each Windows version. This is an informational change only. 5.1 02/13/2019 08:00:00 In the Security Updates table, corrected the Servicing Stack Update (SSU) for Windows 10 Version 1809 for x64-based Systems to 4470788. This is an informational change only. 6.0 03/12/2019 07:00:00 A Servicing Stack Update has been released for Windows 7 and Windows Server 2008 R2 and Windows Server 2008 R2 (Server Core installation). See the FAQ section for more information. 8.0 05/14/2019 07:00:00 A Servicing Stack Update has been released for Windows 10 version 1507, Windows 10 version 1607, Windows Server 2016, Windows 10 version 1703, Windows 10 version 1709, Windows Server, version 1709, Windows 10 version 1803, Windows Server, version 1803, Windows 10 version 1809, Windows Server 2019, Windows 10 version 1809 and Windows Server, version 1809. See the FAQ section for more information. 9.0 06/11/2019 07:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	A Servicing Stack Update has been released for Windows 10 version 1607, Windows Server 2016, Windows 10 version 1809, and Windows Server 2019. See the FAQ section for more information. 10.0 06/14/2019 07:00:00 A Servicing Stack Update has been released for Windows 10 version 1903 and Windows Server, version 1903 (Server Core installation). See the FAQ section for more information. 13.0 07/26/2019 07:00:00 A Servicing Stack Update has been released for Windows 10 version 1903 and Windows Server, version 1903 (Server Core installation). See the FAQ section for more information. 14.0 09/10/2019 07:00:00 A Servicing Stack Update has been released for all supported versions of Windows. See the FAQ section for more information. 15.0 10/08/2019 07:00:00 A Servicing Stack Update has been released for all supported versions of Windows 10 (including Windows Server 2016 and 2019), Windows 8.1, Windows Server 2012 R2 and Windows Server 2012. See the FAQ section for more information. 15.1 10/09/2019 07:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	In the Security Updates table, corrected the KB Article Number and Download links for Server 2012, the 32-bit and x64-based versions of Windows 8.1, and Server 2012 R2. See the FAQ section for more information. 16.0 11/12/2019 08:00:00 A Servicing Stack Update has been released for all supported versions of Windows. See the FAQ section for more information. 1.0 11/13/2018 08:00:00 Information published. 1.1 11/14/2018 08:00:00 Corrected the link to the Windows Server 2008 Servicing Stack Update. This is an informational change only. 2.0 12/05/2018 08:00:00 A Servicing Stack Update has been released for Windows 10 Version 1809 and Windows Server 2019. See the FAQ section for more information. 3.0 12/11/2018 08:00:00 A Servicing Stack Update has been released for Windows 10 Version 1709, Windows Server, version 1709 (Server Core Installation), Windows 10 Version 1803, and Windows Server, version 1803 (Server Core Installation). See the FAQ section for more information. 3.1 12/11/2018 08:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Updated supersedence information. This is an informational change only. 3.2 12/12/2018 08:00:00 Fixed a typo in the FAQ. 4.0 01/08/2019 08:00:00 A Servicing Stack Update has been released for Windows 10 Version 1703. See the FAQ section for more information. 5.0 02/12/2019 08:00:00 A Servicing Stack Update has been released for Windows 10 Version 1607, Windows Server 2016, and Windows Server 2016 (Server Core installation); Windows 10 Version 1703; Windows 10 Version 1709 and Windows Server, version 1709 (Server Core Installation); Windows 10 Version 1803, and Windows Server, version 1803 (Server Core Installation). See the FAQ section for more information. 5.2 02/14/2019 08:00:00 In the Security Updates table, corrected the Servicing Stack Update (SSU) for Windows 10 Version 1803 for x64-based Systems to 4485449. This is an informational change only. 7.0 04/09/2019 07:00:00 A Servicing Stack Update has been released for Windows Server 2008 and Windows Server 2008 (Server Core installation); Windows 10 version 1809, Windows Server 2019, and Windows Server 2019 (Server Core installation). See the FAQ section for more information.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	11.0 07/09/2019 07:00:00 A Servicing Stack Update has been released for all supported versions of Windows 10 (including Windows Server 2016 and 2019), Windows 8.1, Windows Server 2012 R2 and Windows Server 2012. See the FAQ section for more information. 12.0 07/24/2019 07:00:00 A Servicing Stack Update has been released for Windows 10 Version 1809 and Windows Server 2019. See the FAQ section for more information. 16.1 11/13/2019 08:00:00 Fixed some incorrect KB numbers. This is an information change only. 17.0 12/10/2019 08:00:00 A Servicing Stack Update has been released for Windows Server 2008 and Windows Server 2008 (Server Core installation); Windows 7, Windows Server 2008 R2, and Windows Server 2008 R2 (Server Core installation). See the FAQ section for more information.		

Affected Software

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

ADV990001						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4523203 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for x64-based Systems	4523203 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server, version 1803 (Server Core Installation)	4523203 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for ARM64-based Systems	4523203 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1809 for 32-bit Systems	4523204 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes

ADV990001						
Windows 10 Version 1809 for x64-based Systems	4523204 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1809 for ARM64-based Systems	4523204 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2019	4523204 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2019 (Server Core installation)	4523204 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for 32-bit Systems	4523202 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for x64-based Systems	4523202 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal:	Yes

ADV990001						
					N/A Vector: N/A	
Windows 10 Version 1709 for ARM64-based Systems	4523202 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 for 32-bit Systems	4523200 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 for x64-based Systems	4523200 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1607 for 32-bit Systems	4520724 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1607 for x64-based Systems	4520724 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes

ADV990001						
Windows Server 2016	4520724 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2016 (Server Core installation)	4520724 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 7 for 32-bit Systems Service Pack 1	4523206 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 7 for x64-based Systems Service Pack 1	4523206 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 8.1 for 32-bit systems	4524445 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 8.1 for x64-based systems	4524445 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal:	Yes

ADV990001						
					N/A Vector: N/A	
Windows Server 2008 for 32-bit Systems Service Pack 2	4526478 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4526478 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4526478 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4526478 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4526478 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes

ADV990001						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4523206 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4523206 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4523206 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012	4523208 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 (Server Core installation)	4523208 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 R2	4524445 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal:	Yes

ADV990001						
					N/A Vector: N/A	
Windows Server 2012 R2 (Server Core installation)	4524445 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1903 for ARM64-based Systems	4524569 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1903 for 32-bit Systems	4524569 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1903 for x64-based Systems	4524569 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server, version 1903 (Server Core installation)	4524569 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1332 - Microsoft SQL Server Reporting Services XSS Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1332 MITRE NVD	**CVE Title:** Microsoft SQL Server Reporting Services XSS Vulnerability **Description:** A cross-site scripting (XSS) vulnerability exists when Microsoft SQL Server Reporting Services (SSRS) does not properly sanitize a specially-crafted web request to an affected SSRS server. An attacker who successfully exploited the vulnerability could run scripts in the context of the targeted user. The attacks could allow the attacker to read content that the attacker is not authorized to read, execute malicious code, and use the victim's identity to take actions on the site on behalf of the user, such as change permissions and delete content. To exploit the vulnerability, an attacker would need to convince an authenticated user to click a specially-crafted link to an affected SSRS server. The update addresses the vulnerability by correcting SSRS URL sanitization. **FAQ:** None	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1332						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
SQL Server 2017 Reporting Services	Release Notes Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1332						
Power BI Report Server	Release Notes Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Yes
SQL Server 2019 Reporting Services	Release Notes Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1349 - Git for Visual Studio Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1349 MITRE NVD	**CVE Title:** Git for Visual Studio Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when Git for Visual Studio improperly sanitizes input. 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 accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, an attacker would first need to convince the user to clone a malicious repo. The security update addresses the vulnerability by correcting how Git for Visual Studio validates command-line input. **FAQ:** **I want to install the latest supported service baseline for Visual Studio. Do I need to install the previous versions first?** No. For both Visual Studio 2019 and Visual Studio 2017, the latest supported servicing baseline is cumulative. For example, if you need to install Visual Studio 2019 version 16.4 you do NOT first have to install any previous versions. See Visual Studio 2019 version 16.4 Release Notes for more information. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00		

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

Affected Software

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

CVE-2019-1349						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Visual Studio 2017 version 15.9 (includes 15.1 - 15.8)	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Visual Studio 2017 version 15.0	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1349						
Microsoft Visual Studio 2019 version 16.0	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1350 - Git for Visual Studio Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1350 MITRE NVD	**CVE Title:** Git for Visual Studio Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when Git for Visual Studio improperly sanitizes input. 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 accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, an attacker would first need to convince the user to clone a malicious repo. The security update addresses the vulnerability by correcting how Git for Visual Studio validates command-line input. **FAQ:** **I want to install the latest supported service baseline for Visual Studio. Do I need to install the previous versions first?** No. For both Visual Studio 2019 and Visual Studio 2017, the latest supported servicing baseline is cumulative. For example, if you need to install Visual Studio 2019 version 16.4 you do NOT first have to install any previous versions. See Visual Studio 2019 version 16.4 Release Notes for more information. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00		

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

Affected Software

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

CVE-2019-1350						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Visual Studio 2017 version 15.9 (includes 15.1 - 15.8)	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1350						
Microsoft Visual Studio 2017 version 15.0	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Visual Studio 2019 version 16.0	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1351 - Git for Visual Studio Tampering Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1351 MITRE NVD	**CVE Title:** Git for Visual Studio Tampering Vulnerability **Description:** A tampering vulnerability exists when Git for Visual Studio improperly handles virtual drive paths. An attacker who successfully exploited this vulnerability could write arbitrary files and directories to certain locations on a vulnerable system. However, an attacker would have limited control over the destination of the files and directories.	Moderate	Tampering

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, an attacker must clone a file using a specially crafted path on a vulnerable system. The security update fixes the vulnerability by ensuring Git for Visual Studio properly handles folder paths. **FAQ:** **I want to install the latest supported service baseline for Visual Studio. Do I need to install the previous versions first?** No. For both Visual Studio 2019 and Visual Studio 2017, the latest supported servicing baseline is cumulative. For example, if you need to install Visual Studio 2019 version 16.4 you do NOT first have to install any previous versions. See Visual Studio 2019 version 16.4 Release Notes for more information. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00		

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

Affected Software

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

CVE-2019-1351						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Visual Studio 2017 version 15.9 (includes 15.1 - 15.8)	Release Notes Security Update	Moderate	Tampering		Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Visual Studio 2017 version 15.0	Release Notes Security Update	Moderate	Tampering		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1351						
Microsoft Visual Studio 2017 version 16.0	Release Notes Security Update	Moderate	Tampering		Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)	Release Notes Security Update	Moderate	Tampering		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1352 - Git for Visual Studio Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1352 MITRE NVD	**CVE Title:** Git for Visual Studio Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when Git for Visual Studio improperly sanitizes input. 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 accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, an attacker would first need to convince the user to clone a malicious repo. The security update addresses the vulnerability by correcting how Git for Visual Studio validates command-line input. **FAQ:** **I want to install the latest supported service baseline for Visual Studio. Do I need to install the previous versions first?** No. For both Visual Studio 2019 and Visual Studio 2017, the latest supported servicing baseline is cumulative. For example, if you need to install Visual Studio 2019 version 16.4 you do NOT first have to install any previous versions. See Visual Studio 2019 version 16.4 Release Notes for more information. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00		

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

Affected Software

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

CVE-2019-1352						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Visual Studio 2017 version 15.9 (includes 15.1 - 15.8)	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1352						
Microsoft Visual Studio 2017 version 15.0	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Visual Studio 2019 version 16.0	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1354 - Git for Visual Studio Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1354 MITRE NVD	**CVE Title:** Git for Visual Studio Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when Git for Visual Studio improperly sanitizes input. 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 accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, an attacker would first need to convince the user to clone a malicious repo. The security update addresses the vulnerability by correcting how Git for Visual Studio validates command-line input. **FAQ:** **I want to install the latest supported service baseline for Visual Studio. Do I need to install the previous versions first?** No. For both Visual Studio 2019 and Visual Studio 2017, the latest supported servicing baseline is cumulative. For example, if you need to install Visual Studio 2019 version 16.4 you do NOT first have to install any previous versions. See Visual Studio 2019 version 16.4 Release Notes for more information. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00		

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

Affected Software

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

CVE-2019-1354						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Visual Studio 2017 version 15.9 (includes 15.1 - 15.8)	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1354						
Microsoft Visual Studio 2017 version 15.0	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Visual Studio 2019 version 16.0	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1387 - Git for Visual Studio Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1387 MITRE NVD	**CVE Title:** Git for Visual Studio Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when Git for Visual Studio improperly sanitizes input. 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 accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, an attacker would first need to convince the user to clone a malicious repo. The security update addresses the vulnerability by correcting how Git for Visual Studio validates command-line input. **FAQ:** **I want to install the latest supported service baseline for Visual Studio. Do I need to install the previous versions first?** No. For both Visual Studio 2019 and Visual Studio 2017, the latest supported servicing baseline is cumulative. For example, if you need to install Visual Studio 2019 version 16.4 you do NOT first have to install any previous versions. See Visual Studio 2019 version 16.4 Release Notes for more information. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00		

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

Affected Software

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

CVE-2019-1387						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Visual Studio 2017 version 15.9 (includes 15.1 - 15.8)	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1387						
Microsoft Visual Studio 2017 version 15.0	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Visual Studio 2019 version 16.0	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1400 - Microsoft Access Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1400 MITRE NVD	**CVE Title:** Microsoft Access Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in Microsoft Access software when the software fails to properly handle objects in memory. An attacker who successfully exploited this 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 the 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 Microsoft Access 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 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1400						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2019 for 32-bit editions	Click to Run Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Office 2019 for 64-bit editions	Click to Run Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Yes
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Yes
Office 365 ProPlus for 64-bit Systems	Click to Run Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1400						
Microsoft Office 2016 (32-bit edition)	4484180 Security Update	Important	Information Disclosure	4484113	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Office 2016 (64-bit edition)	4484180 Security Update	Important	Information Disclosure	4484113	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4484193 Security Update	Important	Information Disclosure	4484127	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4484193 Security Update	Important	Information Disclosure	4484127	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Office 2013 RT Service Pack 1	4484186 Security Update	Important	Information Disclosure	4484119	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4484186 Security Update	Important	Information Disclosure	4484119	Base: N/A Temporal:	Yes

CVE-2019-1400						
					N/A Vector: N/A	
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4484186 Security Update	Important	Information Disclosure	4484119	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1453 - Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1453 MITRE NVD	**CVE Title:** Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability **Description:** A denial of service vulnerability exists in Remote Desktop Protocol (RDP) 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 RDP service on the target system to stop responding.	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit this vulnerability, an attacker would need to run a specially crafted application against a server which provides Remote Desktop Protocol (RDP) services. The update addresses the vulnerability by correcting how RDP handles connection requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1453						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1909 for 32-bit Systems	4530684 Security Update	Important	Denial of Service	4524570	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4530684 Security Update	Important	Denial of Service	4524570	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4530684 Security Update	Important	Denial of Service	4524570	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4530684 Security Update	Important	Denial of Service	4524570	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4530717 Security Update	Important	Denial of Service	4525237	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1453						
Windows 10 Version 1803 for x64-based Systems	4530717 Security Update	Important	Denial of Service	4525237	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4530717 Security Update	Important	Denial of Service	4525237	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4530717 Security Update	Important	Denial of Service	4525237	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4530715 Security Update	Important	Denial of Service	4523205	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4530715 Security Update	Important	Denial of Service	4523205	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1453						
Windows 10 Version 1809 for ARM64-based Systems	4530715 Security Update	Important	Denial of Service	4523205	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4530715 Security Update	Important	Denial of Service	4523205	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4530715 Security Update	Important	Denial of Service	4523205	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4530714 Security Update	Important	Denial of Service	4525241	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4530714 Security Update	Important	Denial of Service	4525241	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709	4530714 Security	Important	Denial of Service	4525241	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-1453						
for ARM64-based Systems	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 10 Version 1903 for 32-bit Systems	4530684 Security Update	Important	Denial of Service	4524570	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4530684 Security Update	Important	Denial of Service	4524570	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4530684 Security Update	Important	Denial of Service	4524570	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4530684 Security Update	Important	Denial of Service	4524570	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4530681 Security Update	Important	Denial of Service	4525232	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1453						
Windows 10 for x64-based Systems	4530681 Security Update	Important	Denial of Service	4525232	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4530689 Security Update	Important	Denial of Service	4525236	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4530689 Security Update	Important	Denial of Service	4525236	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4530689 Security Update	Important	Denial of Service	4525236	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4530689 Security Update	Important	Denial of Service	4525236	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for 32-bit Systems Service Pack 1	4530734 Monthly Rollup	Important	Denial of Service	4525235	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-1453						
	4530692 Security Only				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 7 for x64-based Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Denial of Service	4525235	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4530702 Monthly Rollup 4530730 Security Only	Important	Denial of Service	4525243	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4530702 Monthly Rollup 4530730 Security	Important	Denial of Service	4525243	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1453						
	Only					
Windows RT 8.1	4530702 Monthly Rollup	Important	Denial of Service	4525243	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Denial of Service	4525235	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Denial of Service	4525235	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-	4530734 Monthly Rollup	Important	Denial of Service	4525235	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-1453						
based Systems Service Pack 1 (Server Core installation)	4530692 Security Only				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 2012	4530691 Monthly Rollup 4530698 Security Only	Important	Denial of Service	4525246	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4530691 Monthly Rollup 4530698 Security Only	Important	Denial of Service	4525246	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4530702 Monthly Rollup 4530730 Security	Important	Denial of Service	4525243	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1453						
	Only					
Windows Server 2012 R2 (Server Core installation)	4530702 Monthly Rollup 4530730 Security Only	Important	Denial of Service	4525243	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1458 - Win32k Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1458 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 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1458						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4530681 Security Update	Important	Elevation of Privilege	4525232	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4530681 Security Update	Important	Elevation of Privilege	4525232	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4530689 Security Update	Important	Elevation of Privilege	4525236	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4530689 Security Update	Important	Elevation of Privilege	4525236	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2016	4530689 Security Update	Important	Elevation of Privilege	4525236	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes

CVE-2019-1458						
Windows Server 2016 (Server Core installation)	4530689 Security Update	Important	Elevation of Privilege	4525236	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows 7 for 32-bit Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Elevation of Privilege	4525235	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Elevation of Privilege	4525235	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4530702 Monthly Rollup 4530730 Security	Important	Elevation of Privilege	4525243	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes

CVE-2019-1458						
	Only					
Windows 8.1 for x64-based systems	4530702 Monthly Rollup 4530730 Security Only	Important	Elevation of Privilege	4525243	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows RT 8.1	4530702 Monthly Rollup	Important	Elevation of Privilege	4525243	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4530695 Monthly Rollup 4530719 Security Only	Important	Elevation of Privilege	4525234	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit	4530695 Monthly Rollup	Important	Elevation of Privilege	4525234	Base: 7.8 Temporal: 7.2	Yes

CVE-2019-1458						
Systems Service Pack 2 (Server Core installation)	4530719 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4530695 Monthly Rollup 4530719 Security Only	Important	Elevation of Privilege	4525234	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4530695 Monthly Rollup 4530719 Security Only	Important	Elevation of Privilege	4525234	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4530695 Monthly Rollup 4530719	Important	Elevation of Privilege	4525234	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes

CVE-2019-1458						
Service Pack 2 (Server Core installation)	Security Only					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Elevation of Privilege	4525235	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Elevation of Privilege	4525235	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based	4530734 Monthly Rollup 4530692	Important	Elevation of Privilege	4525235	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes

CVE-2019-1458						
Systems Service Pack 1 (Server Core installation)	Security Only					
Windows Server 2012	4530691 Monthly Rollup 4530698 Security Only	Important	Elevation of Privilege	4525246	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4530691 Monthly Rollup 4530698 Security Only	Important	Elevation of Privilege	4525246	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2012 R2	4530702 Monthly Rollup 4530730	Important	Elevation of Privilege	4525243	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes

CVE-2019-1458						
	Security Only					
Windows Server 2012 R2 (Server Core installation)	4530702 Monthly Rollup 4530730 Security Only	Important	Elevation of Privilege	4525243	Base: 7.8 Temporal: 7.2 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes

CVE-2019-1461 - Microsoft Word Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1461 MITRE NVD	**CVE Title:** Microsoft Word Denial of Service Vulnerability **Description:** A denial of service vulnerability exists in Microsoft Word software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could cause a remote denial of service against a system.	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Exploitation of the vulnerability requires that a specially crafted document be sent to a vulnerable user. The security update addresses the vulnerability by correcting how Microsoft Word handles objects in memory. **FAQ:** **I have Microsoft Word 2010 installed. Why am I not being offered the 4475598 update?** The 4475598 update only applies to systems running specific configurations of Microsoft Office 2010. Some configurations will not be offered the update. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1461						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2019 for 32-bit editions	Click to Run Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Office 2019 for 64-bit editions	Click to Run Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Yes
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Yes
Office 365 ProPlus for 64-bit Systems	Click to Run Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1461						
Microsoft Word 2016 (32-bit edition)	4484169 Security Update	Important	Denial of Service	4475540	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Word 2016 (64-bit edition)	4484169 Security Update	Important	Denial of Service	4475540	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4475598 Security Update	Important	Denial of Service	4475531	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4475598 Security Update	Important	Denial of Service	4475531	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Word 2010 Service Pack 2 (32-bit editions)	4475601 Security Update	Important	Denial of Service	4475533	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Word 2010 Service Pack 2 (64-bit editions)	4475601 Security Update	Important	Denial of Service	4475533	Base: N/A Temporal:	Yes

CVE-2019-1461						
					N/A Vector: N/A	
Microsoft Word 2013 RT Service Pack 1	4484094 Security Update	Important	Denial of Service	4475547	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Word 2013 Service Pack 1 (32-bit editions)	4484094 Security Update	Important	Denial of Service	4475547	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Word 2013 Service Pack 1 (64-bit editions)	4484094 Security Update	Important	Denial of Service	4475547	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1462 - Microsoft PowerPoint Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1462 MITRE NVD	**CVE Title:** Microsoft PowerPoint Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft PowerPoint 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 PowerPoint 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	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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. Note that the Preview Pane is not an attack vector for this vulnerability. The security update addresses the vulnerability by correcting how Microsoft PowerPoint 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 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1462						
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	Yes
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	Yes
Microsoft Office 2019 for Mac	Release Notes Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Yes
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	Yes

CVE-2019-1462						
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	Yes
Microsoft PowerPoint 2013 Service Pack 1 (32-bit editions)	4461590 Security Update	Important	Remote Code Execution	4461481	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft PowerPoint 2013 Service Pack 1 (64-bit editions)	4461590 Security Update	Important	Remote Code Execution	4461481	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft PowerPoint 2013 RT Service Pack 1	4461590 Security Update	Important	Remote Code Execution	4461481	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft PowerPoint 2016 (32-bit edition)	4484166 Security Update	Important	Remote Code Execution	4461532	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft PowerPoint 2016 (64-bit edition)	4484166 Security Update	Important	Remote Code Execution	4461532	Base: N/A Temporal:	Yes

CVE-2019-1462						
					N/A Vector: N/A	
Microsoft Office 2016 for Mac	Release Notes Security Update	Important	Remote Code Execution	4461532	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft PowerPoint 2010 Service Pack 2 (32-bit editions)	4461613 Security Update	Important	Remote Code Execution	4461521	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft PowerPoint 2010 Service Pack 2 (64-bit editions)	4461613 Security Update	Important	Remote Code Execution	4461521	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1463 - Microsoft Access Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1463 MITRE NVD	**CVE Title:** Microsoft Access Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in Microsoft Access software when the software fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system. To exploit the 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 Microsoft Access 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	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1463						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2019 for 32-bit editions	Click to Run Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1463						
Microsoft Office 2019 for 64-bit editions	Click to Run Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Yes
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Yes
Office 365 ProPlus for 64-bit Systems	Click to Run Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Office 2016 (32-bit edition)	4484180 Security Update	Important	Information Disclosure	4484113	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Office 2016 (64-bit edition)	4484180 Security Update	Important	Information Disclosure	4484113	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4484193 Security Update	Important	Information Disclosure	4484127	Base: N/A Temporal:	Yes

CVE-2019-1463						
					N/A Vector: N/A	
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4484193 Security Update	Important	Information Disclosure	4484127	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Office 2013 RT Service Pack 1	4484186 Security Update	Important	Information Disclosure	4484119	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4484186 Security Update	Important	Information Disclosure	4484119	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4484186 Security Update	Important	Information Disclosure	4484119	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1464 - Microsoft Excel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1464 MITRE NVD	**CVE Title:** Microsoft Excel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory. An attacker who exploited the vulnerability could use the information to compromise the userâ€™s computer or data. To exploit the vulnerability, an attacker could craft a special document file and then convince the user to open it. An attacker must know the memory address location where the object was created. The update addresses the vulnerability by changing the way certain Excel functions handle 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	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1464						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2019 for 32-bit editions	Click to Run Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1464						
Microsoft Office 2019 for 64-bit editions	Click to Run Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Office 2019 for Mac	Release Notes Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Yes
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Yes
Office 365 ProPlus for 64-bit Systems	Click to Run Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Excel 2016 (32-bit edition)	4484179 Security Update	Important	Information Disclosure	4484144	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Excel 2016 (64-bit edition)	4484179 Security Update	Important	Information Disclosure	4484144	Base: N/A Temporal:	Yes

CVE-2019-1464						
					N/A Vector: N/A	
Microsoft Office 2016 (32-bit edition)	4484182 Security Update	Important	Information Disclosure	4484148	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Office 2016 (64-bit edition)	4484182 Security Update	Important	Information Disclosure	4484148	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Office 2016 for Mac	Release Notes Security Update	Important	Information Disclosure	4484148	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Excel 2010 Service Pack 2 (32-bit editions)	4484196 Security Update	Important	Information Disclosure	4484164	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Excel 2010 Service Pack 2 (64-bit editions)	4484196 Security Update	Important	Information Disclosure	4484164	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1464						
Microsoft Excel 2013 RT Service Pack 1	4484190 Security Update	Important	Information Disclosure	4484158	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Excel 2013 Service Pack 1 (32-bit editions)	4484190 Security Update	Important	Information Disclosure	4484158	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Excel 2013 Service Pack 1 (64-bit editions)	4484190 Security Update	Important	Information Disclosure	4484158	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4484192 Security Update	Important	Information Disclosure	4484160	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4484192 Security Update	Important	Information Disclosure	4484160	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Office 2013 RT Service Pack 1	4484184 Security Update	Important	Information Disclosure	4484152	Base: N/A Temporal:	Yes

CVE-2019-1464						
					N/A Vector: N/A	
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4484184 Security Update	Important	Information Disclosure	4484152	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4484184 Security Update	Important	Information Disclosure	4484152	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1465 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1465 MITRE NVD	**CVE Title:** Windows GDI Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how the Windows GDI component handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1465						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1909 for ARM64-based Systems	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1465						
Windows 10 Version 1909 for 32-bit Systems	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4530717 Security Update	Important	Information Disclosure	4525237	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4530717 Security Update	Important	Information Disclosure	4525237	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4530717 Security Update	Important	Information Disclosure	4525237	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-	4530717 Security Update	Important	Information Disclosure	4525237	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1465						
based Systems						
Windows 10 Version 1809 for 32-bit Systems	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS: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 2019	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS: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 2019	4530715 Security	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5	Yes

CVE-2019-1465						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1709 for 32-bit Systems	4530714 Security Update	Important	Information Disclosure	4525241	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4530714 Security Update	Important	Information Disclosure	4525241	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4530714 Security Update	Important	Information Disclosure	4525241	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530684 Security	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5	Yes

CVE-2019-1465						
1903 for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1903 for ARM64-based Systems	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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)	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530681 Security Update	Important	Information Disclosure	4525232	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4530681 Security Update	Important	Information Disclosure	4525232	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1465						
Windows 10 Version 1607 for 32-bit Systems	4530689 Security Update	Important	Information Disclosure	4525236	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4530689 Security Update	Important	Information Disclosure	4525236	Base: 5.5 Temporal: 5 Vector: CVSS: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 2016	4530689 Security Update	Important	Information Disclosure	4525236	Base: 5.5 Temporal: 5 Vector: CVSS: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 2016 (Server Core installation)	4530689 Security Update	Important	Information Disclosure	4525236	Base: 5.5 Temporal: 5 Vector: CVSS: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 32-bit Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1465						
	Only					
Windows 7 for x64-based Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530702 Monthly Rollup 4530730 Security Only	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4530702 Monthly Rollup 4530730 Security Only	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1465						
Windows RT 8.1	4530702 Monthly Rollup	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530695 Monthly Rollup 4530719 Security Only	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5 Vector: CVSS: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)	4530695 Monthly Rollup 4530719 Security Only	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530695 Monthly Rollup 4530719	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1465						
Systems Service Pack 2	Security Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4530695 Monthly Rollup 4530719 Security Only	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5 Vector: CVSS: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)	4530695 Monthly Rollup 4530719 Security Only	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5 Vector: CVSS: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-	4530734 Monthly Rollup 4530692	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1465						
Based Systems Service Pack 1	Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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)	4530734 Monthly Rollup 4530692 Security Only	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530691 Monthly Rollup	Important	Information Disclosure	4525246	Base: 5.5 Temporal: 5	Yes

CVE-2019-1465						
	4530698 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 2012 (Server Core installation)	4530691 Monthly Rollup 4530698 Security Only	Important	Information Disclosure	4525246	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4530702 Monthly Rollup 4530730 Security Only	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4530702 Monthly Rollup 4530730 Security	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1465						
	Only					

CVE-2019-1466 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1466 MITRE NVD	**CVE Title:** Windows GDI Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how the Windows GDI component handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1466						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-1466						
Windows 10 Version 1803 for 32-bit Systems	4530717 Security Update	Important	Information Disclosure	4525237	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4530717 Security Update	Important	Information Disclosure	4525237	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4530717 Security Update	Important	Information Disclosure	4525237	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4530717 Security Update	Important	Information Disclosure	4525237	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530715 Security	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5	Yes

CVE-2019-1466						
1809 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS: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 2019	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS: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 2019 (Server Core installation)	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530714 Security	Important	Information Disclosure	4525241	Base: 5.5 Temporal: 5	Yes

CVE-2019-1466						
1709 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1709 for x64-based Systems	4530714 Security Update	Important	Information Disclosure	4525241	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4530714 Security Update	Important	Information Disclosure	4525241	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1466						
Windows 10 Version 1903 for ARM64-based Systems	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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)	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530681 Security Update	Important	Information Disclosure	4525232	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4530681 Security Update	Important	Information Disclosure	4525232	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4530689 Security Update	Important	Information Disclosure	4525236	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1466						
Windows 10 Version 1607 for x64-based Systems	4530689 Security Update	Important	Information Disclosure	4525236	Base: 5.5 Temporal: 5 Vector: CVSS: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 2016	4530689 Security Update	Important	Information Disclosure	4525236	Base: 5.5 Temporal: 5 Vector: CVSS: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 2016 (Server Core installation)	4530689 Security Update	Important	Information Disclosure	4525236	Base: 5.5 Temporal: 5 Vector: CVSS: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 32-bit Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530734 Monthly Rollup	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5	Yes

CVE-2019-1466						
Systems Service Pack 1	4530692 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4530702 Monthly Rollup 4530730 Security Only	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4530702 Monthly Rollup 4530730 Security Only	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4530702 Monthly Rollup	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1466						
Windows Server 2008 for 32-bit Systems Service Pack 2	4530695 Monthly Rollup 4530719 Security Only	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5 Vector: CVSS: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)	4530695 Monthly Rollup 4530719 Security Only	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530695 Monthly Rollup 4530719 Security Only	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1466						
Windows Server 2008 for x64-based Systems Service Pack 2	4530695 Monthly Rollup 4530719 Security Only	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5 Vector: CVSS: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)	4530695 Monthly Rollup 4530719 Security Only	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530734 Monthly Rollup 4530692 Security Only	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1466						
Service Pack 1						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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)	4530734 Monthly Rollup 4530692 Security Only	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530691 Monthly Rollup 4530698 Security	Important	Information Disclosure	4525246	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1466						
	Only					
Windows Server 2012 (Server Core installation)	4530691 Monthly Rollup 4530698 Security Only	Important	Information Disclosure	4525246	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4530702 Monthly Rollup 4530730 Security Only	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4530702 Monthly Rollup 4530730 Security Only	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1466						
Windows 10 Version 1909 for 32-bit Systems	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1467 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1467 MITRE NVD	**CVE Title:** Windows GDI Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how the Windows GDI component handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory. **Mitigations:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1467						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server, version 1909 (Server Core installation)	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1467						
Windows 10 Version 1909 for ARM64-based Systems	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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 32-bit Systems	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4530717 Security Update	Important	Information Disclosure	4525237	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for	4530717 Security Update	Important	Information Disclosure	4525237	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1467						
x64-based Systems						
Windows Server, version 1803 (Server Core Installation)	4530717 Security Update	Important	Information Disclosure	4525237	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4530717 Security Update	Important	Information Disclosure	4525237	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1467						
Windows 10 Version 1809 for ARM64-based Systems	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS: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 2019	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS: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 2019 (Server Core installation)	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4530714 Security Update	Important	Information Disclosure	4525241	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4530714 Security Update	Important	Information Disclosure	4525241	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1467						
Windows 10 Version 1709 for ARM64-based Systems	4530714 Security Update	Important	Information Disclosure	4525241	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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,	4530684 Security	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5	Yes

CVE-2019-1467						
version 1903 (Server Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 for 32-bit Systems	4530681 Security Update	Important	Information Disclosure	4525232	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4530681 Security Update	Important	Information Disclosure	4525232	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4530689 Security Update	Important	Information Disclosure	4525236	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4530689 Security Update	Important	Information Disclosure	4525236	Base: 5.5 Temporal: 5 Vector: CVSS: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 2016	4530689 Security	Important	Information Disclosure	4525236	Base: 5.5 Temporal: 5	Yes

CVE-2019-1467						
	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 2016 (Server Core installation)	4530689 Security Update	Important	Information Disclosure	4525236	Base: 5.5 Temporal: 5 Vector: CVSS: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 32-bit Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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 Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530702 Monthly Rollup	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5	Yes

CVE-2019-1467						
	4530730 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 8.1 for x64-based systems	4530702 Monthly Rollup 4530730 Security Only	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4530702 Monthly Rollup	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530695 Monthly Rollup 4530719 Security Only	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1467						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4530695 Monthly Rollup 4530719 Security Only	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530695 Monthly Rollup 4530719 Security Only	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530695 Monthly Rollup 4530719 Security Only	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1467						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4530695 Monthly Rollup 4530719 Security Only	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5 Vector: CVSS: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 Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530734 Monthly Rollup 4530692 Security	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1467						
Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4530734 Monthly Rollup 4530692 Security Only	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530691 Monthly Rollup 4530698 Security Only	Important	Information Disclosure	4525246	Base: 5.5 Temporal: 5 Vector: CVSS: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 (Server Core installation)	4530691 Monthly Rollup 4530698 Security	Important	Information Disclosure	4525246	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1467						
	Only					
Windows Server 2012 R2	4530702 Monthly Rollup 4530730 Security Only	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4530702 Monthly Rollup 4530730 Security Only	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1468 - Win32k Graphics Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1468 MITRE NVD	**CVE Title:** Win32k Graphics Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. An attacker who successfully exploited this vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. There are multiple ways an attacker could exploit this vulnerability. • In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit this vulnerability and then convince a user to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to click a link in an email message or in an Instant Messenger message that takes users to the attacker's website, or by opening an attachment sent through email.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	• In a file sharing attack scenario, an attacker could provide a specially crafted document file that is designed to exploit this vulnerability, and then convince a user to open the document file. The security update addresses the vulnerability by correcting how the Windows font library handles embedded fonts. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1468						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1909 for x64-based Systems	4530684 Security Update	Critical	Remote Code Execution	4524570	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4530684 Security Update	Critical	Remote Code Execution	4524570	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for 32-bit Systems	4530684 Security Update	Critical	Remote Code Execution	4524570	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909	4530684 Security	Critical	Remote Code Execution	4524570	Base: 8.4 Temporal: 7.6	Yes

CVE-2019-1468						
for ARM64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1803 for 32-bit Systems	4530717 Security Update	Critical	Remote Code Execution	4525237	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4530717 Security Update	Critical	Remote Code Execution	4525237	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4530717 Security Update	Critical	Remote Code Execution	4525237	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4530717 Security Update	Critical	Remote Code Execution	4525237	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4530715 Security Update	Critical	Remote Code Execution	4523205	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1468						
Windows 10 Version 1809 for x64-based Systems	4530715 Security Update	Critical	Remote Code Execution	4523205	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4530715 Security Update	Critical	Remote Code Execution	4523205	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4530715 Security Update	Critical	Remote Code Execution	4523205	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4530715 Security Update	Critical	Remote Code Execution	4523205	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4530714 Security Update	Critical	Remote Code Execution	4525241	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709	4530714 Security	Critical	Remote Code Execution	4525241	Base: 8.4 Temporal: 7.6	Yes

CVE-2019-1468						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1709 for ARM64-based Systems	4530714 Security Update	Critical	Remote Code Execution	4525241	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4530684 Security Update	Critical	Remote Code Execution	4524570	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4530684 Security Update	Critical	Remote Code Execution	4524570	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4530684 Security Update	Critical	Remote Code Execution	4524570	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4530684 Security Update	Critical	Remote Code Execution	4524570	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1468						
Windows 10 for 32-bit Systems	4530681 Security Update	Critical	Remote Code Execution	4525232	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4530681 Security Update	Critical	Remote Code Execution	4525232	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4530689 Security Update	Critical	Remote Code Execution	4525236	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4530689 Security Update	Critical	Remote Code Execution	4525236	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4530689 Security Update	Critical	Remote Code Execution	4525236	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4530689 Security	Critical	Remote Code Execution	4525236	Base: 8.4 Temporal: 7.6	Yes

CVE-2019-1468						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 7 for 32-bit Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Critical	Remote Code Execution	4525235	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/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	4530734 Monthly Rollup 4530692 Security Only	Critical	Remote Code Execution	4525235	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4530702 Monthly Rollup 4530730 Security Only	Critical	Remote Code Execution	4525243	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1468						
Windows 8.1 for x64-based systems	4530702 Monthly Rollup 4530730 Security Only	Critical	Remote Code Execution	4525243	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4530702 Monthly Rollup	Critical	Remote Code Execution	4525243	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/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	4530695 Monthly Rollup 4530719 Security Only	Critical	Remote Code Execution	4525234	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/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	4530695 Monthly Rollup 4530719 Security	Critical	Remote Code Execution	4525234	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1468						
2 (Server Core installation)	Only					
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4530695 Monthly Rollup 4530719 Security Only	Critical	Remote Code Execution	4525234	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/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	4530695 Monthly Rollup 4530719 Security Only	Critical	Remote Code Execution	4525234	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/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	4530695 Monthly Rollup 4530719 Security	Critical	Remote Code Execution	4525234	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1468						
Core installation)	Only					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Critical	Remote Code Execution	4525235	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Critical	Remote Code Execution	4525235	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server	4530734 Monthly Rollup 4530692 Security	Critical	Remote Code Execution	4525235	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1468						
Core installation)	Only					
Windows Server 2012	4530691 Monthly Rollup 4530698 Security Only	Critical	Remote Code Execution	4525246	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4530691 Monthly Rollup 4530698 Security Only	Critical	Remote Code Execution	4525246	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4530702 Monthly Rollup 4530730 Security Only	Critical	Remote Code Execution	4525243	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1468						
Windows Server 2012 R2 (Server Core installation)	4530702 Monthly Rollup 4530730 Security Only	Critical	Remote Code Execution	4525243	Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1469 - Win32k Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1469 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. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how 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 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1469						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4530717 Security Update	Important	Information Disclosure	4525237	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4530717 Security Update	Important	Information Disclosure	4525237	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4530717 Security Update	Important	Information Disclosure	4525237	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530717 Security	Important	Information Disclosure	4525237	Base: 5.5 Temporal: 5	Yes

CVE-2019-1469						
1803 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 10 Version 1809 for 32-bit Systems	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS: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 2019	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1469						
Windows Server 2019 (Server Core installation)	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4530714 Security Update	Important	Information Disclosure	4525241	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4530714 Security Update	Important	Information Disclosure	4525241	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4530714 Security Update	Important	Information Disclosure	4525241	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1469						
Windows 10 Version 1903 for x64-based Systems	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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)	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530681 Security Update	Important	Information Disclosure	4525232	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-	4530681 Security	Important	Information Disclosure	4525232	Base: 5.5 Temporal: 5	Yes

CVE-2019-1469						
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 10 Version 1607 for 32-bit Systems	4530689 Security Update	Important	Information Disclosure	4525236	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4530689 Security Update	Important	Information Disclosure	4525236	Base: 5.5 Temporal: 5 Vector: CVSS: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 2016	4530689 Security Update	Important	Information Disclosure	4525236	Base: 5.5 Temporal: 5 Vector: CVSS: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 2016 (Server Core installation)	4530689 Security Update	Important	Information Disclosure	4525236	Base: 5.5 Temporal: 5 Vector: CVSS: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 32-bit Systems	4530734 Monthly Rollup 4530692	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1469						
Service Pack 1	Security Only					
Windows 7 for x64-based Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530702 Monthly Rollup 4530730 Security Only	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4530702 Monthly Rollup 4530730 Security	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1469						
	Only					
Windows RT 8.1	4530702 Monthly Rollup	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530695 Monthly Rollup 4530719 Security Only	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5 Vector: CVSS: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)	4530695 Monthly Rollup 4530719 Security Only	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530695 Monthly	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5	Yes

CVE-2019-1469						
for Itanium-Based Systems Service Pack 2	Rollup 4530719 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 x64-based Systems Service Pack 2	4530695 Monthly Rollup 4530719 Security Only	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5 Vector: CVSS: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)	4530695 Monthly Rollup 4530719 Security Only	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530734 Monthly	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5	Yes

CVE-2019-1469						
R2 for Itanium-Based Systems Service Pack 1	Rollup 4530692 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 R2 for x64-based Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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)	4530734 Monthly Rollup 4530692 Security Only	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1469						
Windows Server 2012	4530691 Monthly Rollup 4530698 Security Only	Important	Information Disclosure	4525246	Base: 5.5 Temporal: 5 Vector: CVSS: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 (Server Core installation)	4530691 Monthly Rollup 4530698 Security Only	Important	Information Disclosure	4525246	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4530702 Monthly Rollup 4530730 Security Only	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530702 Monthly	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5	Yes

CVE-2019-1469						
R2 (Server Core installation)	Rollup 4530730 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 10 Version 1909 for 32-bit Systems	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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-	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1469						
based Systems						

CVE-2019-1470 - Windows Hyper-V Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1470 MITRE NVD	**CVE Title:** Windows Hyper-V Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system. To exploit the vulnerability, an attacker on a guest operating system could run a specially crafted application that could cause the Hyper-V host operating system to disclose memory information. An attacker who successfully exploited the vulnerability could gain access to information on the Hyper-V host operating system. The security update addresses the vulnerability by correcting how Hyper-V validates guest operating system user input. **FAQ:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	What type of information could be disclosed by this vulnerability? The type of information that could be disclosed if an attacker successfully exploited this vulnerability is the contents of Kernel memory. An attacker could read the contents of Kernel memory from a user mode process. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1470						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for x64-based Systems	4530717 Security Update	Important	Information Disclosure	4525237	Base: 6 Temporal: 5.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4530717 Security Update	Important	Information Disclosure	4525237	Base: 6 Temporal: 5.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4530715 Security Update	Important	Information Disclosure	4523205	Base: 6 Temporal: 5.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4530715 Security Update	Important	Information Disclosure	4523205	Base: 6 Temporal: 5.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1470						
Windows Server 2019 (Server Core installation)	4530715 Security Update	Important	Information Disclosure	4523205	Base: 6 Temporal: 5.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4530714 Security Update	Important	Information Disclosure	4525241	Base: 6 Temporal: 5.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4530684 Security Update	Important	Information Disclosure	4524570	Base: 6 Temporal: 5.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4530684 Security Update	Important	Information Disclosure	4524570	Base: 6 Temporal: 5.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-	4530681 Security	Important	Information Disclosure	4525232	Base: 6 Temporal: 5.4	Yes

CVE-2019-1470						
based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1607 for x64-based Systems	4530689 Security Update	Important	Information Disclosure	4525236	Base: 6 Temporal: 5.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4530689 Security Update	Important	Information Disclosure	4525236	Base: 6 Temporal: 5.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4530689 Security Update	Important	Information Disclosure	4525236	Base: 6 Temporal: 5.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Information Disclosure	4525235	Base: 6 Temporal: 5.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1470						
Windows 8.1 for x64-based systems	4530702 Monthly Rollup 4530730 Security Only	Important	Information Disclosure	4525243	Base: 6 Temporal: 5.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4530695 Monthly Rollup 4530719 Security Only	Important	Information Disclosure	4525234	Base: 6 Temporal: 5.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/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)	4530695 Monthly Rollup 4530719 Security Only	Important	Information Disclosure	4525234	Base: 6 Temporal: 5.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1470						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Information Disclosure	4525235	Base: 6 Temporal: 5.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/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)	4530734 Monthly Rollup 4530692 Security Only	Important	Information Disclosure	4525235	Base: 6 Temporal: 5.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4530691 Monthly Rollup 4530698 Security Only	Important	Information Disclosure	4525246	Base: 6 Temporal: 5.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1470						
Windows Server 2012 (Server Core installation)	4530691 Monthly Rollup 4530698 Security Only	Important	Information Disclosure	4525246	Base: 6 Temporal: 5.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4530702 Monthly Rollup 4530730 Security Only	Important	Information Disclosure	4525243	Base: 6 Temporal: 5.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4530702 Monthly Rollup 4530730 Security Only	Important	Information Disclosure	4525243	Base: 6 Temporal: 5.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server,	4530684 Security	Important	Information Disclosure	4524570	Base: 6 Temporal: 5.4	Yes

CVE-2019-1470						
version 1909 (Server Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1909 for x64-based Systems	4530684 Security Update	Important	Information Disclosure	4524570	Base: 6 Temporal: 5.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1471 - Windows Hyper-V Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1471 MITRE NVD	**CVE Title:** Windows Hyper-V Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system. To exploit the vulnerability, an attacker could run a specially crafted application on a guest operating system that could cause the Hyper-V host operating system to execute arbitrary code.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	An attacker who successfully exploited the vulnerability could execute arbitrary code on the host operating system. The security update addresses the vulnerability by correcting how Hyper-V validates guest operating system user input. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1471						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for x64-based Systems	4530717 Security Update	Critical	Remote Code Execution	4525237	Base: 8.2 Temporal: 7.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4530717 Security Update	Critical	Remote Code Execution	4525237	Base: 8.2 Temporal: 7.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4530715 Security Update	Critical	Remote Code Execution	4523205	Base: 8.2 Temporal: 7.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4530715 Security Update	Critical	Remote Code Execution	4523205	Base: 8.2 Temporal: 7.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4530715 Security Update	Critical	Remote Code Execution	4523205	Base: 8.2 Temporal: 7.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1471						
Windows 10 Version 1903 for x64-based Systems	4530684 Security Update	Critical	Remote Code Execution	4524570	Base: 8.2 Temporal: 7.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4530684 Security Update	Critical	Remote Code Execution	4524570	Base: 8.2 Temporal: 7.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4530684 Security Update	Critical	Remote Code Execution	4524570	Base: 8.2 Temporal: 7.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4530684 Security Update	Critical	Remote Code Execution	4524570	Base: 8.2 Temporal: 7.4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1472 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1472 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system. The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The type of information that could be disclosed if an attacker successfully exploited this vulnerability is the contents of Kernel memory. An attacker could read the contents of Kernel memory from a user mode process. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1472						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1909 for 32-bit Systems	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1472						
Core installation)						
Windows 10 Version 1803 for 32-bit Systems	4530717 Security Update	Important	Information Disclosure	4525237	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4530717 Security Update	Important	Information Disclosure	4525237	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4530717 Security Update	Important	Information Disclosure	4525237	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-	4530717 Security Update	Important	Information Disclosure	4525237	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1472						
based Systems						
Windows 10 Version 1809 for 32-bit Systems	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS: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 2019	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS: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 2019	4530715 Security	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5	Yes

CVE-2019-1472						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1709 for 32-bit Systems	4530714 Security Update	Important	Information Disclosure	4525241	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4530714 Security Update	Important	Information Disclosure	4525241	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4530714 Security Update	Important	Information Disclosure	4525241	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1472						
Windows 10 Version 1903 for x64-based Systems	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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)	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530681 Security Update	Important	Information Disclosure	4525232	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1472						
Windows 10 for x64-based Systems	4530681 Security Update	Important	Information Disclosure	4525232	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4530689 Security Update	Important	Information Disclosure	4525236	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4530689 Security Update	Important	Information Disclosure	4525236	Base: 5.5 Temporal: 5 Vector: CVSS: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 2016	4530689 Security Update	Important	Information Disclosure	4525236	Base: 5.5 Temporal: 5 Vector: CVSS: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 2016 (Server Core installation)	4530689 Security Update	Important	Information Disclosure	4525236	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1474 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1474 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system. The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The type of information that could be disclosed if an attacker successfully exploited this vulnerability is Kernel memory read - unintentional read access to memory contents in kernel space from a user mode process. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1474						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4530717 Security Update	Important	Information Disclosure	4525237	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4530717 Security Update	Important	Information Disclosure	4525237	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4530717 Security Update	Important	Information Disclosure	4525237	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4530717 Security Update	Important	Information Disclosure	4525237	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1474						
Windows 10 Version 1809 for 32-bit Systems	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS: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 2019	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS: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 2019 (Server Core installation)	4530715 Security Update	Important	Information Disclosure	4523205	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1474						
Windows 10 Version 1709 for 32-bit Systems	4530714 Security Update	Important	Information Disclosure	4525241	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4530714 Security Update	Important	Information Disclosure	4525241	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4530714 Security Update	Important	Information Disclosure	4525241	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1474						
x64-based Systems						
Windows 10 Version 1903 for ARM64-based Systems	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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)	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530681 Security Update	Important	Information Disclosure	4525232	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4530681 Security Update	Important	Information Disclosure	4525232	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530689 Security	Important	Information Disclosure	4525236	Base: 5.5 Temporal: 5	Yes

CVE-2019-1474						
1607 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1607 for x64-based Systems	4530689 Security Update	Important	Information Disclosure	4525236	Base: 5.5 Temporal: 5 Vector: CVSS: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 2016	4530689 Security Update	Important	Information Disclosure	4525236	Base: 5.5 Temporal: 5 Vector: CVSS: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 2016 (Server Core installation)	4530689 Security Update	Important	Information Disclosure	4525236	Base: 5.5 Temporal: 5 Vector: CVSS: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 32-bit Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1474						
Windows 7 for x64-based Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530702 Monthly Rollup 4530730 Security Only	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4530702 Monthly Rollup 4530730 Security Only	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4530702 Monthly	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5	Yes

CVE-2019-1474						
	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	4530695 Monthly Rollup 4530719 Security Only	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5 Vector: CVSS: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)	4530695 Monthly Rollup 4530719 Security Only	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530695 Monthly Rollup 4530719 Security	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1474						
Service Pack 2	Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4530695 Monthly Rollup 4530719 Security Only	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5 Vector: CVSS: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)	4530695 Monthly Rollup 4530719 Security Only	Important	Information Disclosure	4525234	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530734 Monthly Rollup 4530692 Security	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1474						
Systems Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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)	4530734 Monthly Rollup 4530692 Security Only	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530691 Monthly Rollup 4530698	Important	Information Disclosure	4525246	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1474						
	Security Only					
Windows Server 2012 (Server Core installation)	4530691 Monthly Rollup 4530698 Security Only	Important	Information Disclosure	4525246	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4530702 Monthly Rollup 4530730 Security Only	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4530702 Monthly Rollup 4530730 Security	Important	Information Disclosure	4525243	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1474						
	Only					
Windows 10 Version 1909 for 32-bit Systems	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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	4530684 Security Update	Important	Information Disclosure	4524570	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1476 - Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1476 MITRE NVD	**CVE Title:** Windows Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links. An attacker who successfully exploited this vulnerability could run processes in an elevated context. An attacker could then install programs; view, change or delete data. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The security update addresses the vulnerability by correcting how Windows AppX Deployment Service handles hard links. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1476						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1909 for ARM64-based Systems	4530684 Security Update	Important	Elevation of Privilege	4524570	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1476						
Windows 10 Version 1909 for 32-bit Systems	4530684 Security Update	Important	Elevation of Privilege	4524570	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4530684 Security Update	Important	Elevation of Privilege	4524570	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4530684 Security Update	Important	Elevation of Privilege	4524570	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4530717 Security Update	Important	Elevation of Privilege	4525237	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4530717 Security Update	Important	Elevation of Privilege	4525237	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1476						
Windows Server, version 1803 (Server Core Installation)	4530717 Security Update	Important	Elevation of Privilege	4525237	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4530717 Security Update	Important	Elevation of Privilege	4525237	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4530715 Security Update	Important	Elevation of Privilege	4523205	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4530715 Security Update	Important	Elevation of Privilege	4523205	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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 ARM64-based Systems	4530715 Security Update	Important	Elevation of Privilege	4523205	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1476						
Windows Server 2019	4530715 Security Update	Important	Elevation of Privilege	4523205	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 (Server Core installation)	4530715 Security Update	Important	Elevation of Privilege	4523205	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4530714 Security Update	Important	Elevation of Privilege	4525241	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4530714 Security Update	Important	Elevation of Privilege	4525241	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4530684 Security Update	Important	Elevation of Privilege	4524570	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1476						
Windows 10 Version 1903 for x64-based Systems	4530684 Security Update	Important	Elevation of Privilege	4524570	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4530684 Security Update	Important	Elevation of Privilege	4524570	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4530684 Security Update	Important	Elevation of Privilege	4524570	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4530689 Security Update	Important	Elevation of Privilege	4525236	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4530689 Security Update	Important	Elevation of Privilege	4525236	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1476						
Windows Server 2016	4530689 Security Update	Important	Elevation of Privilege	4525236	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4530689 Security Update	Important	Elevation of Privilege	4525236	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1477 - Windows Printer Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1477 MITRE NVD	**CVE Title:** Windows Printer Service Elevation of Privilege Vulnerability **Description:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	An elevation of privilege vulnerability exists when the Windows Printer Service improperly validates file paths while loading printer drivers. An authenticated attacker who successfully exploited this vulnerability could run arbitrary code with elevated system privileges. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how the Windows Printer Service validates file paths. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1477						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1809 for 32-bit Systems	4530715 Security Update	Important	Elevation of Privilege	4523205	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4530715 Security Update	Important	Elevation of Privilege	4523205	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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 ARM64-based Systems	4530715 Security Update	Important	Elevation of Privilege	4523205	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4530715 Security	Important	Elevation of Privilege	4523205	Base: 7.8 Temporal: 7	Yes

CVE-2019-1477						
	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2019 (Server Core installation)	4530715 Security Update	Important	Elevation of Privilege	4523205	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1478 - Windows COM Server Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1478 MITRE NVD	**CVE Title:** Windows COM Server Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Windows improperly handles COM object creation. An attacker who successfully exploited the vulnerability could run arbitrary code with elevated privileges. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The update addresses the vulnerability by correcting how the Windows COM Server creates COM objects. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1478						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Elevation of Privilege	4525235	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4530734 Monthly Rollup 4530692 Security Only	Important	Elevation of Privilege	4525235	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4530695 Monthly Rollup 4530719 Security Only	Important	Elevation of Privilege	4525234	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1478						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4530695 Monthly Rollup 4530719 Security Only	Important	Elevation of Privilege	4525234	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4530695 Monthly Rollup 4530719 Security Only	Important	Elevation of Privilege	4525234	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4530695 Monthly Rollup 4530719 Security Only	Important	Elevation of Privilege	4525234	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1478						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4530695 Monthly Rollup 4530719 Security Only	Important	Elevation of Privilege	4525234	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4530734 Monthly Rollup 4530692 Security Only	Important	Elevation of Privilege	4525235	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4530734 Monthly Rollup 4530692 Security Only	Important	Elevation of Privilege	4525235	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1478						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4530734 Monthly Rollup 4530692 Security Only	Important	Elevation of Privilege	4525235	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1480 - Windows Media Player Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1480 MITRE NVD	**CVE Title:** Windows Media Player Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in Windows Media Player 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.	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 open a specifically crafted file. The update addresses the vulnerability by correcting how Windows Media Player 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 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1480						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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 Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1481 - Windows Media Player Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1481 MITRE NVD	**CVE Title:** Windows Media Player Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in Windows Media Player 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. To exploit this vulnerability, an attacker would have to log on to an affected system and open a specifically crafted file. The update addresses the vulnerability by correcting how Windows Media Player 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.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1481						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems	4530734 Monthly Rollup	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5	Yes

CVE-2019-1481						
Service Pack 1	4530692 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	4530734 Monthly Rollup 4530692 Security Only	Important	Information Disclosure	4525235	Base: 5.5 Temporal: 5 Vector: CVSS: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-2019-1483 - Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1483 MITRE NVD	**CVE Title:** Windows Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows AppX Deployment Server improperly handles junctions.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 AppX Deployment Server handles junctions. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1483						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1909 for ARM64-based Systems	4530684 Security Update	Important	Elevation of Privilege	4524570	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4530684 Security Update	Important	Elevation of Privilege	4524570	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4530684 Security Update	Important	Elevation of Privilege	4524570	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4530684 Security Update	Important	Elevation of Privilege	4524570	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803	4530717 Security	Important	Elevation of Privilege	4525237	Base: 7.8 Temporal: 7	Yes

CVE-2019-1483						
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	4530717 Security Update	Important	Elevation of Privilege	4525237	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4530717 Security Update	Important	Elevation of Privilege	4525237	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4530717 Security Update	Important	Elevation of Privilege	4525237	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4530715 Security Update	Important	Elevation of Privilege	4523205	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4530715 Security	Important	Elevation of Privilege	4523205	Base: 7.8 Temporal: 7	Yes

CVE-2019-1483						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for ARM64-based Systems	4530715 Security Update	Important	Elevation of Privilege	4523205	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4530715 Security Update	Important	Elevation of Privilege	4523205	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 (Server Core installation)	4530715 Security Update	Important	Elevation of Privilege	4523205	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4530714 Security Update	Important	Elevation of Privilege	4525241	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4530714 Security Update	Important	Elevation of Privilege	4525241	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1483						
Windows 10 Version 1709 for ARM64-based Systems	4530714 Security Update	Important	Elevation of Privilege	4525241	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4530684 Security Update	Important	Elevation of Privilege	4524570	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4530684 Security Update	Important	Elevation of Privilege	4524570	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4530684 Security Update	Important	Elevation of Privilege	4524570	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4530684 Security Update	Important	Elevation of Privilege	4524570	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1484 - Windows OLE Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1484 MITRE NVD	**CVE Title:** Windows OLE Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input. An attacker could exploit the vulnerability to execute malicious code. To exploit the vulnerability, an attacker would have to convince a user to open a specially crafted file or a program, causing Windows to execute arbitrary code. The update addresses the vulnerability by correcting how Windows OLE validates user input. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00	Important	Remote Code Execution

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

Affected Software

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

CVE-2019-1484						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4530717 Security Update	Important	Remote Code Execution	4525237	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4530717 Security Update	Important	Remote Code Execution	4525237	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1484						
Windows Server, version 1803 (Server Core Installation)	4530717 Security Update	Important	Remote Code Execution	4525237	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4530717 Security Update	Important	Remote Code Execution	4525237	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4530715 Security Update	Important	Remote Code Execution	4523205	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4530715 Security Update	Important	Remote Code Execution	4523205	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4530715 Security Update	Important	Remote Code Execution	4523205	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1484						
Windows Server 2019	4530715 Security Update	Important	Remote Code Execution	4523205	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4530715 Security Update	Important	Remote Code Execution	4523205	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4530714 Security Update	Important	Remote Code Execution	4525241	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4530714 Security Update	Important	Remote Code Execution	4525241	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4530714 Security Update	Important	Remote Code Execution	4525241	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1484						
Windows 10 Version 1903 for 32-bit Systems	4530684 Security Update	Important	Remote Code Execution	4524570	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4530684 Security Update	Important	Remote Code Execution	4524570	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4530684 Security Update	Important	Remote Code Execution	4524570	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4530684 Security Update	Important	Remote Code Execution	4524570	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4530681 Security Update	Important	Remote Code Execution	4525232	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1484						
Windows 10 for x64-based Systems	4530681 Security Update	Important	Remote Code Execution	4525232	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4530689 Security Update	Important	Remote Code Execution	4525236	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4530689 Security Update	Important	Remote Code Execution	4525236	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4530689 Security Update	Important	Remote Code Execution	4525236	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4530689 Security Update	Important	Remote Code Execution	4525236	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for 32-bit Systems	4530734 Monthly Rollup	Important	Remote Code Execution	4525235	Base: 7.8 Temporal: 7	Yes

CVE-2019-1484						
Service Pack 1	4530692 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 7 for x64-based Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Remote Code Execution	4525235	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4530702 Monthly Rollup 4530730 Security Only	Important	Remote Code Execution	4525243	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4530702 Monthly Rollup 4530730 Security	Important	Remote Code Execution	4525243	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1484						
	Only					
Windows RT 8.1	4530702 Monthly Rollup	Important	Remote Code Execution	4525243	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4530695 Monthly Rollup 4530719 Security Only	Important	Remote Code Execution	4525234	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4530695 Monthly Rollup 4530719 Security Only	Important	Remote Code Execution	4525234	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1484						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4530695 Monthly Rollup 4530719 Security Only	Important	Remote Code Execution	4525234	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4530695 Monthly Rollup 4530719 Security Only	Important	Remote Code Execution	4525234	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4530695 Monthly Rollup 4530719 Security Only	Important	Remote Code Execution	4525234	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1484						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Remote Code Execution	4525235	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Remote Code Execution	4525235	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server	4530734 Monthly Rollup 4530692 Security Only	Important	Remote Code Execution	4525235	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1484						
Core installation)						
Windows Server 2012	4530691 Monthly Rollup 4530698 Security Only	Important	Remote Code Execution	4525246	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4530691 Monthly Rollup 4530698 Security Only	Important	Remote Code Execution	4525246	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4530702 Monthly Rollup 4530730 Security Only	Important	Remote Code Execution	4525243	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1484						
Windows Server 2012 R2 (Server Core installation)	4530702 Monthly Rollup 4530730 Security Only	Important	Remote Code Execution	4525243	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server Core installation)	4530684 Security Update	Important	Remote Code Execution	4524570	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4530684 Security Update	Important	Remote Code Execution	4524570	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for 32-bit Systems	4530684 Security Update	Important	Remote Code Execution	4524570	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1484						
Windows 10 Version 1909 for x64-based Systems	4530684 Security Update	Important	Remote Code Execution	4524570	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1485 - VBScript Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1485 MITRE NVD	**CVE Title:** VBScript Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1485						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 10 on Windows Server 2012	4530691 Monthly Rollup 4530677 IE Cumulative	Low	Remote Code Execution	4525106	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	4530677 IE Cumulative 4530695 Monthly Rollup	Low	Remote Code Execution	4525234	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-2019-1485						
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4530677 IE Cumulative 4530695 Monthly Rollup	Low	Remote Code Execution	4525234	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	4530717 Security Update	Important	Remote Code Execution	4525237	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	4530717 Security Update	Important	Remote Code Execution	4525237	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-2019-1485						
10 Version 1803 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems	4530717 Security Update	Important	Remote Code Execution	4525237	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1809 for	4530715 Security Update	Important	Remote Code Execution	4523205	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-2019-1485						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4530715 Security Update	Important	Remote Code Execution	4523205	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems	4530715 Security Update	Important	Remote Code Execution	4523205	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-2019-1485						
Internet Explorer 11 on Windows Server 2019	4530715 Security Update	Low	Remote Code Execution	4523205	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 1709 for 32-bit Systems	4530714 Security Update	Important	Remote Code Execution	4525241	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for	4530714 Security Update	Important	Remote Code Execution	4525241	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-2019-1485						
x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems	4530714 Security Update	Important	Remote Code Execution	4525241	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems	4530684 Security Update	Important	Remote Code Execution	4524570	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-2019-1485						
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems	4530684 Security Update	Important	Remote Code Execution	4524570	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	4530684 Security Update	Important	Remote Code Execution	4524570	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	4530681 Security Update	Important	Remote Code Execution	4525232	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-2019-1485						
10 for 32-bit Systems						
Internet Explorer 11 on Windows 10 for x64-based Systems	4530681 Security Update	Important	Remote Code Execution	4525232	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4530689 Security Update	Important	Remote Code Execution	4525236	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	4530689 Security Update	Important	Remote Code Execution	4525236	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-2019-1485						
10 Version 1607 for x64-based Systems						
Internet Explorer 11 on Windows Server 2016	4530689 Security Update	Low	Remote Code Execution	4525236	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 7 for 32-bit Systems Service Pack 1	4530677 IE Cumulative 4530734 Monthly Rollup	Important	Remote Code Execution	4525235	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	4530677 IE Cumulative 4530734	Important	Remote Code Execution	4525235	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-1485						
Windows 7 for x64-based Systems Service Pack 1	Monthly Rollup				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 8.1 for 32-bit systems	4530677 IE Cumulative 4530702 Monthly Rollup	Important	Remote Code Execution	4525243	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4530677 IE Cumulative 4530702 Monthly Rollup	Important	Remote Code Execution	4525243	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	4530702 Monthly	Important	Remote Code Execution	4525243	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-1485						
Windows RT 8.1	Rollup				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 Server 2008 R2 for x64-based Systems Service Pack 1	4530677 IE Cumulative 4530734 Monthly Rollup	Low	Remote Code Execution	4525235	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012	4530677 IE Cumulative	Low	Remote Code Execution	4525106	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	4530677 IE Cumulative 4530702 Monthly	Low	Remote Code Execution	4525243	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-2019-1485						
Server 2012 R2	Rollup					
Internet Explorer 11 on Windows 10 Version 1909 for 32-bit Systems	4530684 Security Update	Important	Remote Code Execution	4524570	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1909 for ARM64-based Systems	4530684 Security Update	Important	Remote Code Execution	4524570	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-2019-1485						
Internet Explorer 11 on Windows 10 Version 1909 for x64-based Systems	4530684 Security Update	Important	Remote Code Execution	4524570	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-2019-1486 - Visual Studio Live Share Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1486 MITRE NVD	**CVE Title:** Visual Studio Live Share Spoofing Vulnerability **Description:** A spoofing vulnerability exists in Visual Studio Live Share when a guest connected to a Live Share session is redirected to an arbitrary URL specified by the session host. An attacker who successfully exploited this vulnerability could cause a connected guest's computer to open a browser and navigate to a URL without consent from the guest.	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, an attacker would need to host a Live Share session and convince a targeted user to connect to the session. The update addresses the vulnerability by prompting the Live Share guest for consent prior to browsing to the host-specified URL. **FAQ:** **I want to install the latest supported service baseline for Visual Studio. Do I need to install the previous versions first?** No. For both Visual Studio 2019 and Visual Studio 2017, the latest supported servicing baseline is cumulative. For example, if you need to install Visual Studio 2019 version 16.4 you do NOT first have to install any previous versions. See Visual Studio 2019 version 16.4 Release Notes for more information. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00		

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

Affected Software

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

CVE-2019-1486						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)	Release Notes Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Visual Studio Live Share extension	Release Notes Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1486						
Microsoft Visual Studio 2019 version 16.0	Release Notes Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1487 - Microsoft Authentication Library for Android Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1487 MITRE NVD	**CVE Title:** Microsoft Authentication Library for Android Information Disclosure Vulnerability **Description:** An information disclosure vulnerability in Android Apps using Microsoft Authentication Library (MSAL) 0.3.1-Alpha or later exists under specific conditions. This vulnerability could result in sensitive data being exposed. To exploit this vulnerability an attacker would need to be authenticated to have rights to view the sensitive data. This security update addresses the vulnerability by modifying how the data is sanitized.	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 sensitive information. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1487						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Authentication Library (MSAL) for Android	Github Repository Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-1488 - Microsoft Defender Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1488 MITRE NVD	**CVE Title:** Microsoft Defender Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists when Microsoft Defender improperly handles specific buffers. An attacker could exploit the vulnerability to trigger warnings and false positives when no threat is present. To exploit the vulnerability, an attacker would first require execution permissions on the victim system. The security update addresses the vulnerability by ensuring Microsoft Defender properly handles these buffers.	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1488						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-1488						
Windows 10 Version 1803 for 32-bit Systems	4530717 Security Update	Important	Security Feature Bypass	4525237	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4530717 Security Update	Important	Security Feature Bypass	4525237	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4530717 Security Update	Important	Security Feature Bypass	4525237	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4530717 Security Update	Important	Security Feature Bypass	4525237	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4530715 Security Update	Important	Security Feature Bypass	4523205	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1488						
Windows 10 Version 1809 for x64-based Systems	4530715 Security Update	Important	Security Feature Bypass	4523205	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4530715 Security Update	Important	Security Feature Bypass	4523205	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4530715 Security Update	Important	Security Feature Bypass	4523205	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4530715 Security Update	Important	Security Feature Bypass	4523205	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4530714 Security Update	Important	Security Feature Bypass	4525241	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709	4530714 Security	Important	Security Feature Bypass	4525241	Base: 3.3 Temporal: 3	Yes

CVE-2019-1488						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1709 for ARM64-based Systems	4530714 Security Update	Important	Security Feature Bypass	4525241	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4530684 Security Update	Important	Security Feature Bypass	4524570	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4530684 Security Update	Important	Security Feature Bypass	4524570	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4530684 Security Update	Important	Security Feature Bypass	4524570	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4530684 Security Update	Important	Security Feature Bypass	4524570	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1488						
Windows 10 for 32-bit Systems	4530681 Security Update	Important	Security Feature Bypass	4525232	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4530681 Security Update	Important	Security Feature Bypass	4525232	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4530689 Security Update	Important	Security Feature Bypass	4525236	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4530689 Security Update	Important	Security Feature Bypass	4525236	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4530689 Security Update	Important	Security Feature Bypass	4525236	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4530689 Security	Important	Security Feature Bypass	4525236	Base: 3.3 Temporal: 3	Yes

CVE-2019-1488						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	
Windows 7 for 32-bit Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Security Feature Bypass	4525235	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Security Feature Bypass	4525235	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4530702 Monthly Rollup 4530730 Security Only	Important	Security Feature Bypass	4525243	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1488						
Windows 8.1 for x64-based systems	4530702 Monthly Rollup 4530730 Security Only	Important	Security Feature Bypass	4525243	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4530702 Monthly Rollup	Important	Security Feature Bypass	4525243	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4530695 Monthly Rollup 4530719 Security Only	Important	Security Feature Bypass	4525234	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4530695 Monthly Rollup 4530719 Security	Important	Security Feature Bypass	4525234	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1488						
(Server Core installation)	Only					
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4530695 Monthly Rollup 4530719 Security Only	Important	Security Feature Bypass	4525234	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4530695 Monthly Rollup 4530719 Security Only	Important	Security Feature Bypass	4525234	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4530695 Monthly Rollup 4530719 Security Only	Important	Security Feature Bypass	4525234	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1488						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Security Feature Bypass	4525235	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4530734 Monthly Rollup 4530692 Security Only	Important	Security Feature Bypass	4525235	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4530734 Monthly Rollup 4530692 Security Only	Important	Security Feature Bypass	4525235	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1488						
Windows Server 2012	4530691 Monthly Rollup 4530698 Security Only	Important	Security Feature Bypass	4525246	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4530691 Monthly Rollup 4530698 Security Only	Important	Security Feature Bypass	4525246	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4530702 Monthly Rollup 4530730 Security Only	Important	Security Feature Bypass	4525243	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1488						
Windows Server 2012 R2 (Server Core installation)	4530702 Monthly Rollup 4530730 Security Only	Important	Security Feature Bypass	4525243	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for 32-bit Systems	4530684 Security Update	Important	Security Feature Bypass	4524570	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for x64-based Systems	4530684 Security Update	Important	Security Feature Bypass	4524570	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1909 for ARM64-based Systems	4530684 Security Update	Important	Security Feature Bypass	4524570	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1909 (Server	4530684 Security Update	Important	Security Feature Bypass	4524570	Base: 3.3 Temporal: 3 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1488						
Core installation)						

CVE-2019-1489 - Remote Desktop Protocol Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1489 MITRE NVD	**CVE Title:** Remote Desktop Protocol Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows Remote Desktop Protocol (RDP) fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system. To exploit this vulnerability, an attacker would have to connect remotely to an affected system and run a specially crafted application. **FAQ:** **Why is there no update for this vulnerability?**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Microsoft will not provide an update for this vulnerability because Windows XP is out of support. Microsoft strongly recommends upgrading to a supported version of Windows software. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1489						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-1489						
Microsoft Windows XP Service Pack 3		Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	

CVE-2019-1490 - Skype for Business Server Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1490 MITRE NVD	**CVE Title:** Skype for Business Server Spoofing Vulnerability **Description:** A spoofing vulnerability exists when a Skype for Business Server does not properly sanitize a specially crafted request. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected server. The attacker who successfully exploited this vulnerability could then perform cross-site scripting attacks on affected systems and run scripts in the security context of the current user. For the vulnerability to be exploited, a user must click a specially crafted URL that takes the user to a targeted Skype for Business site.	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	In an email attack scenario, an attacker could exploit the vulnerability by sending an email message containing the specially crafted URL to the user of the targeted Skype for Business site and convincing the user to click the specially crafted URL. The security update addresses the vulnerability by helping to ensure that Skype for Business Server properly sanitizes web requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 12/10/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-1490						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Skype for Business Server 2019 CU2	4534761 Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Yes

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.