微软发布 6 月补丁修复 93 个安全问题

安全威胁通告

发布时间：2019 年 6 月 12 日

综述

微软于周二发布了 6 月安全更新补丁，修复了 93 个从简单的欺骗攻击到远程执行代码的安全问题，产品涉及 Adobe Flash Player、Kerberos、Microsoft Browsers、Microsoft Devices、Microsoft Edge、Microsoft Exchange Server、Microsoft Graphics Component、Microsoft JET Database Engine、Microsoft Office、Microsoft Office SharePoint、Microsoft Scripting Engine、Microsoft Windows、Servicing Stack Updates、Skype for Business and Microsoft Lync、Team Foundation Server、VBScript、

Windows Authentication Methods、Windows Hyper-V、Windows IIS、Windows Installer、Windows Kernel、Windows Media、Windows NTLM 以及 Windows Shell。

相关信息如下：

产品	CVE 编号	CVE 标题	严重程度
Adobe Flash Player	ADV190015	June 2019 Adobe Flash 安全更新	Critical
Kerberos	CVE-2019-0972	Local Security Authority Subsystem Service 拒绝服务漏洞	Important
Microsoft Browsers	CVE-2019-1038	Microsoft Browser 内存破坏漏洞	Critical

Microsoft Browsers	CVE-2019-1081	Microsoft Browser 信息泄露漏洞	Important
Microsoft Devices	ADV190016	Bluetooth Low Energy Advisory	Important
Microsoft Devices	ADV190017	Microsoft HoloLens Remote Code Execution Vulnerabilities	Important
Microsoft Edge	CVE-2019-1054	Microsoft Edge 安全功能绕过漏洞	Important
Microsoft Exchange Server	ADV190018	Microsoft Exchange Server Defense in Depth Update	Unknown
Microsoft Graphics Component	CVE-2019-1009	Windows GDI 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-1010	Windows GDI 信息泄露漏洞	Important

Microsoft Graphics Component	CVE-2019-1011	Windows GDI 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-1012	Windows GDI 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-1013	Windows GDI 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-1015	Windows GDI 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-1016	Windows GDI 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-1018	DirectX 特权提升漏洞	Important
Microsoft Graphics Component	CVE-2019-1046	Windows GDI 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-1047	Windows GDI 信息泄露漏洞	Important

Microsoft Graphics Component	CVE-2019-1048	Windows GDI 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-1049	Windows GDI 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-1050	Windows GDI 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-0960	Win32k 特权提升漏洞	Important
Microsoft Graphics Component	CVE-2019-0968	Windows GDI 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-0977	Windows GDI 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-0985	Microsoft Speech API 远程代码执行漏洞	Critical

Microsoft JET Database Engine	CVE-2019-0904	Jet Database Engine 远程代码执行漏洞	Important
Microsoft JET Database Engine	CVE-2019-0905	Jet Database Engine 远程代码执行漏洞	Important
Microsoft JET Database Engine	CVE-2019-0906	Jet Database Engine 远程代码执行漏洞	Important
Microsoft JET Database Engine	CVE-2019-0907	Jet Database Engine 远程代码执行漏洞	Important
Microsoft JET Database Engine	CVE-2019-0908	Jet Database Engine 远程代码执行漏洞	Important
Microsoft JET Database Engine	CVE-2019-0909	Jet Database Engine 远程代码执行漏洞	Important

Microsoft JET Database Engine	CVE-2019-0974	Jet Database Engine 远程代码执行漏洞	Important
Microsoft Office	CVE-2019-1034	Microsoft Word 远程代码执行漏洞	Important
Microsoft Office	CVE-2019-1035	Microsoft Word 远程代码执行漏洞	Important
Microsoft Office SharePoint	CVE-2019-1036	Microsoft Office SharePoint XSS Vulnerability	Important
Microsoft Office SharePoint	CVE-2019-1031	Microsoft Office SharePoint XSS Vulnerability	Important
Microsoft Office SharePoint	CVE-2019-1032	Microsoft Office SharePoint XSS Vulnerability	Important
Microsoft Office SharePoint	CVE-2019-1033	Microsoft Office SharePoint XSS Vulnerability	Important

Microsoft Scripting Engine	CVE-2019-0988	Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-0989	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-1055	Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-0920	Scripting Engine 内存破坏漏洞	Moderate
Microsoft Scripting Engine	CVE-2019-0990	Scripting Engine 信息泄露漏洞	Critical
Microsoft Scripting Engine	CVE-2019-0991	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-0992	Chakra Scripting Engine 内存破坏漏洞	Critical

Microsoft Scripting Engine	CVE-2019-0993	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-1002	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-1003	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-1023	Scripting Engine 信息泄露漏洞	Critical
Microsoft Scripting Engine	CVE-2019-1024	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-1051	Chakra Scripting Engine 内存破坏漏洞	Critical

Microsoft Scripting Engine	CVE-2019-1052	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-1080	Scripting Engine 内存破坏漏洞	Moderate
Microsoft Windows	CVE-2019-0888	ActiveX Data Objects (ADO) 远程代码执行漏洞	Critical
Microsoft Windows	CVE-2019-0943	Windows ALPC 特权提升漏洞	Important
Microsoft Windows	CVE-2019-0948	Windows Event Viewer 信息泄露漏洞	Moderate
Microsoft Windows	CVE-2019-0959	Windows Common Log File System Driver 特权提升漏洞	Important

Microsoft Windows	CVE-2019-0984	Windows Common Log File System Driver 特权提升漏洞	Important
Microsoft Windows	CVE-2019-0709	Windows Hyper-V 远程代码执行漏洞	Critical
Microsoft Windows	CVE-2019-0710	Windows Hyper-V 拒绝服务漏洞	Important
Microsoft Windows	CVE-2019-0711	Windows Hyper-V 拒绝服务漏洞	Important
Microsoft Windows	CVE-2019-0713	Windows Hyper-V 拒绝服务漏洞	Important
Microsoft Windows	CVE-2019-0722	Windows Hyper-V 远程代码执行漏洞	Critical

Microsoft Windows	CVE-2019-0983	Windows Storage Service 特权提升漏洞	Important
Microsoft Windows	CVE-2019-0998	Windows Storage Service 特权提升漏洞	Important
Microsoft Windows	CVE-2019-1025	Windows 拒绝服务漏洞	Important
Microsoft Windows	CVE-2019-1043	Comctl32 远程代码执行漏洞	Important
Microsoft Windows	CVE-2019-1045	Windows Network File System 特权提升漏洞	Important
Microsoft Windows	CVE-2019-1064	Windows 特权提升漏洞	Important
Microsoft Windows	CVE-2019-1069	Task Scheduler 特权提升漏洞	Important

Servicing Stack Updates	ADV990001	Latest Servicing Stack Updates	Critical
Skype for Business and Microsoft Lync	CVE-2019-1029	Skype for Business and Lync Server 拒绝服务漏洞	Important
Team Foundation Server	CVE-2019-0996	Azure DevOps Server 欺骗漏洞	Important
VBScript	CVE-2019-1005	Scripting Engine 内存破坏漏洞	Important
Windows Authentication Methods	CVE-2019-1040	Windows NTLM Tampering Vulnerability	Important
Windows Hyper-V	CVE-2019-0620	Windows Hyper-V 远程代码执行漏洞	Critical
Windows IIS	CVE-2019-0941	Microsoft IIS Server 拒绝服务漏洞	Important

Windows Installer	CVE-2019-0973	Windows Installer 特权提升漏洞	Important
Windows Kernel	CVE-2019-1014	Win32k 特权提升漏洞	Important
Windows Kernel	CVE-2019-1017	Win32k 特权提升漏洞	Important
Windows Kernel	CVE-2019-1039	Windows Kernel 信息泄露漏洞	Important
Windows Kernel	CVE-2019-1041	Windows Kernel 特权提升漏洞	Important
Windows Kernel	CVE-2019-1044	Windows Secure Kernel Mode 安全功能绕过漏洞	Important
Windows Kernel	CVE-2019-1065	Windows Kernel 特权提升漏洞	Important

Windows Media	CVE-2019-1007	Windows Audio Service 特权提升漏洞	Important
Windows Media	CVE-2019-1021	Windows Audio Service 特权提升漏洞	Important
Windows Media	CVE-2019-1022	Windows Audio Service 特权提升漏洞	Important
Windows Media	CVE-2019-1026	Windows Audio Service 特权提升漏洞	Important
Windows Media	CVE-2019-1027	Windows Audio Service 特权提升漏洞	Important
Windows Media	CVE-2019-1028	Windows Audio Service 特权提升漏洞	Important

Windows NTLM	CVE-2019-1019	Microsoft Windows 安全功能绕过漏洞	Important
Windows Shell	CVE-2019-0986	Windows User Profile Service 特权提升漏洞	Important
Windows Shell	CVE-2019-1053	Windows Shell 特权提升漏洞	Important

修复建议

微软官方已经发布更新补丁，请及时进行补丁更新。

附件

ADV190015 - June 2019 Adobe Flash Security Update

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV190015 MITRE NVD	**CVE Title:** June 2019 Adobe Flash Security Update **Description:** This security update addresses the following vulnerability, which is described in Adobe Security Bulletin APSB19-30: CVE-2019-7845. Please note that in the event of any discrepancies. the definitive source of information (for example, vulnerability severity and impact) is the Adobe Flash bulletin as referenced. **FAQ:** **How could an attacker exploit these vulnerabilities?** In a web-based attack scenario where the user is using Internet Explorer for the desktop, an attacker could host a specially crafted website that is designed to exploit any of these vulnerabilities through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 any of these vulnerabilities. In all cases, however, 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 clicking 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. In a web-based attack scenario where the user is using Internet Explorer in the Windows 8-style UI, an attacker would first need to compromise a website already listed in the Compatibility View (CV) list. An attacker could then host a website that contains specially crafted Flash content designed to exploit any of these vulnerabilities through Internet Explorer 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 clicking 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. For more information about Internet Explorer and the CV List, please see the MSDN Article, Developer Guidance for websites with content for Adobe Flash Player in Windows 8.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: **Workarounds:** Workaround refers to a setting or configuration change that would help block known attack vectors before you apply the update. **Prevent Adobe Flash Player from running** You can disable attempts to instantiate Adobe Flash Player in Internet Explorer and other applications that honor the kill bit feature, such as Office 2007 and Office 2010, by setting the kill bit for the control in the registry. **Warning** If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk. To set the kill bit for the control in the registry, perform the following steps: 1. Paste the following into a text file and save it with the .reg file extension. 2. Windows Registry Editor Version 5.00 3. [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}] 4. "Compatibility Flags"=dword:00000400		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	5. 6. [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\ActiveX Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}] 7. "Compatibility Flags"=dword:00000400 8. Double-click the .reg file to apply it to an individual system. You can also apply this workaround across domains by using Group Policy. For more information about Group Policy, see the TechNet article, Group Policy collection. **Note** You must restart Internet Explorer for your changes to take effect. **Impact of workaround**. There is no impact as long as the object is not intended to be used in Internet Explorer. **How to undo the workaround.** Delete the registry keys that were added in implementing this workaround. **Prevent Adobe Flash Player from running in Internet Explorer through Group Policy Note** The Group Policy MMC snap-in can be used to set policy for a machine, for an organizational unit, or for an entire domain. For more information about Group Policy, visit the following Microsoft Web sites: Group Policy Overview What is Group Policy Object Editor? Core Group Policy tools and settings		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To disable Adobe Flash Player in Internet Explorer through Group Policy, perform the following steps: **Note** This workaround does not prevent Flash from being invoked from other applications, such as Microsoft Office 2007 or Microsoft Office 2010. 1. Open the Group Policy Management Console and configure the console to work with the appropriate Group Policy object, such as local machine, OU, or domain GPO. 2. Navigate to the following node: **Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Add-on Management** 3. Double-click **Turn off Adobe Flash in Internet Explorer and prevent applications from using Internet Explorer technology to instantiate Flash objects**. 4. Change the setting to Enabled. 5. Click **Apply** and then click **OK** to return to the Group Policy Management Console. 6. Refresh Group Policy on all systems or wait for the next scheduled Group Policy refresh interval for the settings to take effect. **Prevent Adobe Flash Player from running in Office 2010 on affected systems Note** This workaround does not prevent Adobe Flash Player from running in Internet Explorer. **Warning** If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk. For detailed steps that you can use to prevent a control from running in Internet Explorer, see Microsoft Knowledge Base Article 240797. Follow the steps in the article to create a Compatibility		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Flags value in the registry to prevent a COM object from being instantiated in Internet Explorer. To disable Adobe Flash Player in Office 2010 only, set the kill bit for the ActiveX control for Adobe Flash Player in the registry using the following steps: 1. Create a text file named Disable_Flash.reg with the following contents: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Common\COM\Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}] "Compatibility Flags"=dword:00000400 2. Double-click the .reg file to apply it to an individual system. 3. **Note** You must restart Internet Explorer for your changes to take effect. You can also apply this workaround across domains by using Group Policy. For more information about Group Policy, see the TechNet article, Group Policy collection. **Prevent ActiveX controls from running in Office 2007 and Office 2010** To disable all ActiveX controls in Microsoft Office 2007 and Microsoft Office 2010, including Adobe Flash Player in Internet Explorer, perform the following steps:		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	1. Click File, click Options, click Trust Center, and then click Trust Center Settings. 2. Click ActiveX Settings in the left-hand pane, and then select Disable all controls without notifications. 3. Click OK to save your settings. **Impact of workaround**. Office documents that use embedded ActiveX controls may not display as intended. **How to undo the workaround**. To re-enable ActiveX controls in Microsoft Office 2007 and Microsoft Office 2010, perform the following steps: 1. Click File, click Options, click Trust Center, and then click Trust Center Settings. 2. Click ActiveX Settings in the left-hand pane, and then deselect Disable all controls without notifications. 3. Click OK to save your settings. **Set Internet and Local intranet security zone settings to "High" to block ActiveX Controls and Active Scripting in these zones** You can help protect against exploitation of these vulnerabilities by changing your settings for the Internet security zone to block ActiveX controls and Active Scripting. You can do this by setting your browser security to High. To raise the browsing security level in Internet Explorer, perform the following steps:		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	1. On the Internet Explorer **Tools** menu, click** Internet Option**s. 2. In the **Internet Options** dialog box, click the **Security** tab, and then click **Internet**. 3. Under **Security level for this zone**, move the slider to **High**. This sets the security level for all websites you visit to High. 4. Click **Local intranet**. 5. Under **Security level for this zone**, move the slider to **High**. This sets the security level for all websites you visit to High. 6. Click **OK** to accept the changes and return to Internet Explorer. **Note** If no slider is visible, click **Default Level**, and then move the slider to **High**. **Note** Setting the level to High may cause some websites to work incorrectly. If you have difficulty using a website after you change this setting, and you are sure the site is safe to use, you can add that site to your list of trusted sites. This will allow the site to work correctly even with the security setting set to High. **Impact of workaround**. There are side effects to blocking ActiveX Controls and Active Scripting. Many websites on the Internet or an intranet use ActiveX or Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use ActiveX Controls to provide menus, ordering forms, or even account statements. Blocking ActiveX Controls or Active Scripting is a global setting that affects all Internet and intranet sites. If you do not want to block ActiveX Controls or Active Scripting for such sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone". **Configure Internet Explorer**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone You can help protect against exploitation of these vulnerabilities by changing your settings to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone. To do this, perform the following steps: 1. In Internet Explorer, click **Internet Options** on the **Tools** menu. 2. Click the **Security** tab. 3. Click **Internet**, and then click **Custom Level**. 4. Under **Settings**, in the **Scripting** section, under **Active Scripting**, click **Prompt** or **Disable**, and then click **OK**. 5. Click **Local intranet**, and then click **Custom Level**. 6. Under **Settings**, in the **Scripting** section, under **Active Scripting**, click **Prompt** or **Disable**, and then click **OK**. 7. Click **OK** to return to Internet Explorer, and then click **OK** again. **Note** Disabling Active Scripting in the Internet and Local intranet security zones may cause some websites to work incorrectly. If you have difficulty using a website after you change this setting, and you are sure the site is safe to use, you can add that site to your list of trusted sites. This will allow the site to work correctly. **Impact of workaround**. There are side effects to prompting before running Active Scripting. Many websites that are on the Internet or		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	on an intranet use Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use Active Scripting to provide menus, ordering forms, or even account statements. Prompting before running Active Scripting is a global setting that affects all Internet and intranet sites. You will be prompted frequently when you enable this workaround. For each prompt, if you feel you trust the site that you are visiting, click **Yes** to run Active Scripting. If you do not want to be prompted for all these sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone". **Add sites that you trust to the Internet Explorer Trusted sites zone** After you set Internet Explorer to require a prompt before it runs ActiveX controls and Active Scripting in the Internet zone and in the Local intranet zone, you can add sites that you trust to the Internet Explorer Trusted sites zone. This will allow you to continue to use trusted websites exactly as you do today, while helping to protect you from this attack on untrusted sites. We recommend that you add only sites that you trust to the Trusted sites zone. To do this, perform the following steps: 1. In Internet Explorer, click **Tools**, click **Internet Options**, and then click the **Security** tab. 2. In the **Select a web content zone to specify its current security settings** box, click **Trusted Sites**, and then click **Sites**.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	3. If you want to add sites that do not require an encrypted channel, click to clear the **Require server verification (https:) for all sites in this zone** check box. 4. In the **Add this website to the zone** box, type the URL of a site that you trust, and then click **Add**. 5. Repeat these steps for each site that you want to add to the zone. 6. Click **OK** two times to accept the changes and return to Internet Explorer. **Note** Add any sites that you trust not to take malicious action on your system. Two sites in particular that you may want to add are ***.windowsupdate.microsoft.com** and ***.update.microsoft.com**. These are the sites that will host the update, and they require an ActiveX control to install the update. **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

ADV190015						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Adobe Flash Player on Windows Server 2012	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 8.1 for 32-bit systems	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 8.1 for x64-based systems	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows Server 2012 R2	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows RT 8.1	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV190015						
Adobe Flash Player on Windows 10 for 32-bit Systems	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 for x64-based Systems	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows Server 2016	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1607 for 32-bit Systems	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1607 for x64-based Systems	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1703 for 32-bit Systems	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal:	Yes

ADV190015						
					N/A Vector: N/A	
Adobe Flash Player on Windows 10 Version 1703 for x64-based Systems	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1709 for 32-bit Systems	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1709 for x64-based Systems	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1803 for 32-bit Systems	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1803 for x64-based Systems	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV190015						
Adobe Flash Player on Windows 10 Version 1803 for ARM64-based Systems	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1809 for 32-bit Systems	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1809 for x64-based Systems	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1809 for ARM64-based Systems	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows Server 2019	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1709 for ARM64-based Systems	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal:	Yes

ADV190015						
					N/A Vector: N/A	
Adobe Flash Player on Windows 10 Version 1903 for 32-bit Systems	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1903 for x64-based Systems	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1903 for ARM64-based Systems	4503308 Security Update	Critical	Remote Code Execution	4497932	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV190016 - Bluetooth Low Energy Advisory

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV190016 MITRE NVD	**CVE Title:** Bluetooth Low Energy Advisory **Description:** **Executive Summary** Microsoft is aware of an issue that affects the Bluetooth Low Energy (BLE) version of FIDO Security Keys. Due to a misconfiguration in the Bluetooth pairing protocols, it is possible for an attacker who is physically close to a user at the moment he/she uses the security key to communicate with the security key, or communicate with the device to which the key is paired. Google has issued CVE-2019-2102 for this vulnerability. To address this issue, Microsoft has blocked the pairing of these Bluetooth Low Energy (BLE) keys with the pairing misconfiguration. **Recommended Actions** 1. Microsoft recommends that customers install the June security update for Windows.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	2. Customers using the Bluetooth Low Energy (BLE) version of the Titan Security Key by Google should review Androidâ€™s June Bulletins and Googleâ€™s advisory and take appropriate action. 3. Customers using the Feitian Multipass (Feitian CTAP1/U2F Security Key) should review Feitian's Product Issue Notification website and take appropriate action. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

ADV190016						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Important	Elevation of Privilege	4499171	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Important	Elevation of Privilege	4499171	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 8.1 for 32-bit systems	4503290 Security Only 4503276 Monthly Rollup	Important	Elevation of Privilege	4499151	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security Only	Important	Elevation of Privilege	4499151	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security Only	Important	Elevation of Privilege	4499151	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV190016						
Windows RT 8.1	4503276 Monthly Rollup	Important	Elevation of Privilege	4499151	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Elevation of Privilege	4499151	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 for 32-bit Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2016	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: N/A Temporal:	Yes

ADV190016						
					N/A Vector: N/A	
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2016 (Server Core installation)	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV190016						
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server, version 1803 (Server Core Installation)	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: N/A Temporal:	Yes

ADV190016						
					N/A Vector: N/A	
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2019	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2019 (Server Core installation)	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV190016						
Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: N/A Temporal: N/A Vector: N/A	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: N/A Temporal: N/A Vector: N/A	No

ADV190017 - Microsoft HoloLens Remote Code Execution Vulnerabilities

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV190017 MITRE NVD	**CVE Title:** Microsoft HoloLens Remote Code Execution Vulnerabilities **Description:** **Executive Summary** Microsoft is aware of vulnerabilities that affect the Broadcom wireless chipset included in the Microsoft HoloLens device. The vulnerabilities could allow an unauthenticated attacker in physical proximity to cause a denial of service condition or execute code on a target system. The vulnerabilities were issued CVE-2019-9500, CVE-2019-9501, CVE-2019-9502, and CVE-2019-9503. To address this issue, Microsoft has included the updated Broadcom firmware in the latest HoloLens update. **Recommended Actions** Microsoft recommends that customers install the June security update for HoloLens. See the **Security Updates** table for the link to the update and more information.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

ADV190017						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

ADV190017						
Windows 10 Version 1809 for HoloLens	4503327 Security Update	Important	Remote Code Execution	4494441	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV190018 - Microsoft Exchange Server Defense in Depth Update

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV190018 MITRE NVD	**CVE Title:** Microsoft Exchange Server Defense in Depth Update **Description:** Microsoft has released an update for Microsoft Exchange Server that provides enhanced security as a defense in depth measure. **FAQ:** None **Mitigations:** None **Workarounds:** None	Unknown	Defense in Depth

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

ADV190018						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Exchange Server 2010 Service Pack 3	4503028 Security Update		Defense in Depth	4491413	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2019	4503027 Security Update		Defense in Depth	4487563	Base: N/A Temporal: N/A Vector: N/A	Maybe

ADV190018						
Microsoft Exchange Server 2016 Cumulative Update 11	4503027 Security Update		Defense in Depth	4487563	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2013 Cumulative Update 22	4503028 Security Update		Defense in Depth	4487563	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2016 Cumulative Update 12	4503027 Security Update		Defense in Depth	4487563	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2019 Cumulative Update 1	4503027 Security Update		Defense in Depth	4487563	Base: N/A Temporal: N/A Vector: N/A	Maybe

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 sytem. 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:	Critical	Defense in Depth

CVE ID	Vulnerability Description			Maximum Severity Rating	Vulnerability Impact
	Product	**SSU Package**	**Date Released**		
	Windows Server 2008	4493730	April 2019		
	Windows 7/Server 2008 R2	4490628	March 2019		
	Windows Server 2012	3173426	July 2016		
	Windows 8.1/Server 2012 R2	3173424	July 2016		
	Windows 10	4498353	May 2019		
	Windows 10 Version 1607/Server 2016	4503537	June 2019		
	Windows 10 Version 1703	4500640	May 2019		
	Windows 10 1709/Windows Server, version 1709	4500641	May 2019		
	Windows 10 1803/Windows Server, version 1803	4497398	May 2019		
	Windows 10 1809/Server 2019	4504369	June 2019		
	Windows 10 1903/Windows Server, version 1903	4500109	May 2019		
	Mitigations: None **Workarounds:** None				

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 3.1 12/11/2018 08:00:00 Updated supersedence information. This is an informational change only. 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. 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. 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. 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,		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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. 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. 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. 3.2 12/12/2018 08:00:00 Fixed a typo in the FAQ. 1.2 12/03/2018 08:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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. 9.0 06/11/2019 07:00:00 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. 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. 1.0 11/13/2018 08:00:00 Information published. 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. 5.2 02/14/2019 08:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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.		

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 7 for 32-bit Systems Service Pack 1	4490628 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	4490628 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes

ADV990001						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4490628 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4490628 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	4490628 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)	4493730 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012	3173426 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 (Server Core installation)	3173426 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal:	Yes

ADV990001						
					N/A Vector: N/A	
Windows 8.1 for 32-bit systems	3173424 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 8.1 for x64-based systems	3173424 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 R2	3173424 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 R2 (Server Core installation)	3173424 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 for 32-bit Systems	4498353 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV990001						
Windows 10 for x64-based Systems	4498353 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2016	4503537 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1607 for 32-bit Systems	4503537 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1607 for x64-based Systems	4503537 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2016 (Server Core installation)	4503537 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1703 for 32-bit Systems	4500640 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal:	Yes

ADV990001						
					N/A Vector: N/A	
Windows 10 Version 1703 for x64-based Systems	4500640 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for 32-bit Systems	4500641 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for x64-based Systems	4500641 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for 32-bit Systems	4497398 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for x64-based Systems	4497398 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV990001						
Windows Server, version 1803 (Server Core Installation)	4497398 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for ARM64-based Systems	4497398 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1809 for 32-bit Systems	4504369 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1809 for x64-based Systems	4504369 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1809 for ARM64-based Systems	4504369 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2019	4504369 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal:	Yes

ADV990001						
					N/A Vector: N/A	
Windows Server 2019 (Server Core installation)	4504369 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for ARM64-based Systems	4500641 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1903 for 32-bit Systems	4500109 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1903 for x64-based Systems	4500109 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1903 for ARM64-based Systems	4500109 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV990001						
Windows Server, version 1903 (Server Core installation)	4500109 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4493730 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4493730 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4493730 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4493730 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0620 - Windows Hyper-V Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0620 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. 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0620						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012	4503263 Security Only 4503285	Critical	Remote Code Execution	4499171	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0620						
	Monthly Rollup					
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Critical	Remote Code Execution	4499171	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security Only	Critical	Remote Code Execution	4499151	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security Only	Critical	Remote Code Execution	4499151	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Critical	Remote Code Execution	4499151	Base: 7.6 Temporal: 6.8	Yes

CVE-2019-0620						
					Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Critical	Remote Code Execution	4499151	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0620						
Windows Server 2016 (Server Core installation)	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 7.6 Temporal: 6.8	Yes

CVE-2019-0620						
1803 (Server Core Installation)					Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/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	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0620						
Windows Server 2019	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/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)	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 7.6 Temporal: 6.8	Yes

CVE-2019-0620						
ARM64-based Systems					Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	No

CVE-2019-0709 - Windows Hyper-V Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0709	**CVE Title:** Windows Hyper-V Remote Code Execution Vulnerability **Description:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	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. 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 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0709						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for x64-based Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 7.6 Temporal: 6.8	Yes

CVE-2019-0709						
Core installation)					Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0710 - Windows Hyper-V Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0710 MITRE NVD	**CVE Title:** Windows Hyper-V Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application that causes a host machine to crash. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application. The security update addresses the vulnerability by resolving a number of conditions where Hyper-V would fail to prevent a guest operating system from sending malicious requests. **FAQ:** None **Mitigations:** None	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0710						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security Only	Important	Denial of Service	4499151	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0710						
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security Only	Important	Denial of Service	4499151	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Important	Denial of Service	4499151	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Denial of Service	4499151	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Important	Denial of Service	4499154	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4503267 Security Update	Important	Denial of Service	4494440	Base: 6.8 Temporal: 6.1	Yes

CVE-2019-0710						
					Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Important	Denial of Service	4494440	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4503267 Security Update	Important	Denial of Service	4494440	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Denial of Service	4499181	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Denial of Service	4499179	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0710						
Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Denial of Service	4499167	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4503286 Security Update	Important	Denial of Service	4499167	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Denial of Service	4499167	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Denial of Service	4494441	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-	4503327 Security Update	Important	Denial of Service	4494441	Base: 6.8 Temporal: 6.1	Yes

CVE-2019-0710						
based Systems					Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows Server 2019	4503327 Security Update	Important	Denial of Service	4494441	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4503327 Security Update	Important	Denial of Service	4494441	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Important	Denial of Service	4499179	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0711 - Windows Hyper-V Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0711 MITRE NVD	**CVE Title:** Windows Hyper-V Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application that causes a host machine to crash. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application. The security update addresses the vulnerability by resolving a number of conditions where Hyper-V would fail to prevent a guest operating system from sending malicious requests. **FAQ:** None **Mitigations:** None	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0711						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security Only	Important	Denial of Service	4499151	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0711						
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security Only	Important	Denial of Service	4499151	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Important	Denial of Service	4499151	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Denial of Service	4499151	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Important	Denial of Service	4499154	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4503267 Security Update	Important	Denial of Service	4494440	Base: 6.8 Temporal: 6.1	Yes

CVE-2019-0711						
					Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Important	Denial of Service	4494440	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4503267 Security Update	Important	Denial of Service	4494440	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Denial of Service	4499181	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Denial of Service	4499179	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0711						
Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Denial of Service	4499167	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4503286 Security Update	Important	Denial of Service	4499167	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Denial of Service	4499167	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Denial of Service	4494441	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-	4503327 Security Update	Important	Denial of Service	4494441	Base: 6.8 Temporal: 6.1	Yes

CVE-2019-0711						
based Systems					Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows Server 2019	4503327 Security Update	Important	Denial of Service	4494441	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4503327 Security Update	Important	Denial of Service	4494441	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Important	Denial of Service	4499179	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0713 - Windows Hyper-V Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0713 MITRE NVD	**CVE Title:** Windows Hyper-V Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application that causes a host machine to crash. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application. The security update addresses the vulnerability by resolving a number of conditions where Hyper-V would fail to prevent a guest operating system from sending malicious requests. **FAQ:** None **Mitigations:** None	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0713						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Denial of Service	4499164	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0713						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4503269 Security Only 4503292 Monthly Rollup	Important	Denial of Service	4499164	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Denial of Service	4499164	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems	4503269 Security Only 4503292 Monthly Rollup	Important	Denial of Service	4499164	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0713						
Service Pack 1						
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Important	Denial of Service	4499171	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Important	Denial of Service	4499171	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security Only	Important	Denial of Service	4499151	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4503276 Monthly Rollup	Important	Denial of Service	4499151	Base: 6.8 Temporal: 6.1	Yes

CVE-2019-0713						
	4503290 Security Only				Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows RT 8.1	4503276 Monthly Rollup	Important	Denial of Service	4499151	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Denial of Service	4499151	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Important	Denial of Service	4499154	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4503267 Security Update	Important	Denial of Service	4494440	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0713						
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Important	Denial of Service	4494440	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4503267 Security Update	Important	Denial of Service	4494440	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Denial of Service	4499181	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Denial of Service	4499179	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-	4503286 Security Update	Important	Denial of Service	4499167	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0713						
based Systems						
Windows Server, version 1803 (Server Core Installation)	4503286 Security Update	Important	Denial of Service	4499167	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Denial of Service	4499167	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Denial of Service	4494441	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Important	Denial of Service	4494441	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0713						
Windows Server 2019	4503327 Security Update	Important	Denial of Service	4494441	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4503327 Security Update	Important	Denial of Service	4494441	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Important	Denial of Service	4499179	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Important	Denial of Service	4499149	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-	4503273 Monthly Rollup	Important	Denial of Service	4499149	Base: 6.8 Temporal: 6.1	Yes

CVE-2019-0713						
based Systems Service Pack 2	4503287 Security Only				Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Denial of Service	4499149	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0722 - Windows Hyper-V Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0722 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. 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0722						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for x64-based Systems	4503269 Security Only 4503292	Critical	Remote Code Execution	4499164	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0722						
Service Pack 1	Monthly Rollup					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4503269 Security Only 4503292 Monthly Rollup	Critical	Remote Code Execution	4499164	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/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	4503269 Security Only 4503292 Monthly Rollup	Critical	Remote Code Execution	4499164	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/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	4503269 Security Only 4503292	Critical	Remote Code Execution	4499164	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0722						
Systems Service Pack 1	Monthly Rollup					
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Critical	Remote Code Execution	4499171	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Critical	Remote Code Execution	4499171	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security Only	Critical	Remote Code Execution	4499151	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0722						
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security Only	Critical	Remote Code Execution	4499151	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Critical	Remote Code Execution	4499151	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Critical	Remote Code Execution	4499151	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 8.8 Temporal: 7.9	Yes

CVE-2019-0722						
					Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/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)	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/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	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0722						
Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/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)	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/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	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/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	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0722						
Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/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)	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/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	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/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	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 8.8 Temporal: 7.9	No

CVE-2019-0722						
x64-based Systems					Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/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)	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Critical	Remote Code Execution	4499149	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/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-	4503273 Monthly Rollup	Critical	Remote Code Execution	4499149	Base: 8.8 Temporal: 7.9	Yes

CVE-2019-0722						
based Systems Service Pack 2	4503287 Security Only				Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Critical	Remote Code Execution	4499149	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0888 - ActiveX Data Objects (ADO) Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0888 MITRE NVD	**CVE Title:** ActiveX Data Objects (ADO) Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that ActiveX Data Objects (ADO) handle objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary code with the victim userâ€™s privileges. An attacker could craft a website that exploits the vulnerability and then convince a victim user to visit the website. The security update addresses the vulnerability by modifying how ActiveX Data Objects handle objects in memory. **FAQ:** None **Mitigations:** None	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0888						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Critical	Remote Code Execution	4499164	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0888						
Windows 7 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Critical	Remote Code Execution	4499164	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4503269 Security Only 4503292 Monthly Rollup	Critical	Remote Code Execution	4499164	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Critical	Remote Code Execution	4499164	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0888						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Critical	Remote Code Execution	4499164	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Critical	Remote Code Execution	4499149	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Critical	Remote Code Execution	4499171	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0888						
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Critical	Remote Code Execution	4499171	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4503290 Security Only 4503276 Monthly Rollup	Critical	Remote Code Execution	4499151	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security Only	Critical	Remote Code Execution	4499151	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security	Critical	Remote Code Execution	4499151	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0888						
	Only					
Windows RT 8.1	4503276 Monthly Rollup	Critical	Remote Code Execution	4499151	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Critical	Remote Code Execution	4499151	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0888						
Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0888						
Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0888						
Core Installation)						
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0888						
Windows Server 2019	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No

CVE-2019-0888						
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Critical	Remote Code Execution	4499149	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems	4503273 Monthly Rollup 4503287	Critical	Remote Code Execution	4499149	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0888						
Service Pack 2	Security Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Critical	Remote Code Execution	4499149	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Critical	Remote Code Execution	4499149	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0904 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0904 MITRE NVD	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** **Are Active Directory and Exchange Server affected by this vulnerability?** No, Active Directory and Exchange Server are not affected.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0904						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0904						
	Rollup					
Windows 7 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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 Core installation)	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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 Itanium-Based Systems	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0904						
Service Pack 1						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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)	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503263 Security Only 4503285 Monthly	Important	Remote Code Execution	4499171	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0904						
	Rollup					
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Important	Remote Code Execution	4499171	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503290 Security Only 4503276 Monthly Rollup	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503276 Monthly Rollup 4503290 Security Only	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503276 Monthly Rollup 4503290	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0904						
	Security Only					
Windows RT 8.1	4503276 Monthly Rollup	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503291 Security Update	Important	Remote Code Execution	4499154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Important	Remote Code Execution	4499154	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7	Yes

CVE-2019-0904						
					Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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)	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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 1703 for 32-bit Systems	4503279 Security Update	Important	Remote Code Execution	4499181	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0904						
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Remote Code Execution	4499181	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 7.8 Temporal: 7 Vector: CVSS: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 32-bit Systems	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7	Yes

CVE-2019-0904						
x64-based Systems					Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7	Yes

CVE-2019-0904						
x64-based Systems					Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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)	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0904						
Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.8 Temporal: 7 Vector: CVSS: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)	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No

CVE-2019-0904						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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-	4503273 Monthly Rollup	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7	Yes

CVE-2019-0904						
based Systems Service Pack 2 (Server Core installation)	4503287 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	

CVE-2019-0905 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0905 MITRE NVD	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** **Are Active Directory and Exchange Server affected by this vulnerability?** No, Active Directory and Exchange Server are not affected. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0905						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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 x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503269 Security Only 4503292	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0905						
Systems Service Pack 1 (Server Core installation)	Monthly Rollup					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0905						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503263 Security Only 4503285 Monthly Rollup	Important	Remote Code Execution	4499171	Base: 7.8 Temporal: 7 Vector: CVSS: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)	4503263 Security Only 4503285 Monthly Rollup	Important	Remote Code Execution	4499171	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0905						
Windows 8.1 for 32-bit systems	4503290 Security Only 4503276 Monthly Rollup	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503276 Monthly Rollup 4503290 Security Only	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503276 Monthly Rollup 4503290 Security Only	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0905						
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503291 Security Update	Important	Remote Code Execution	4499154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Important	Remote Code Execution	4499154	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0905						
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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)	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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 1703 for 32-bit Systems	4503279 Security Update	Important	Remote Code Execution	4499181	Base: 7.8 Temporal: 7 Vector: CVSS: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 1703 for x64-based Systems	4503279 Security Update	Important	Remote Code Execution	4499181	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 7.8 Temporal: 7	Yes

CVE-2019-0905						
32-bit Systems					Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 7.8 Temporal: 7 Vector: CVSS: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 32-bit Systems	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0905						
Core Installation)						
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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-	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0905						
based Systems						
Windows Server 2019	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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)	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0905						
Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.8 Temporal: 7 Vector: CVSS: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)	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows Server 2008 for Itanium-Based Systems	4503287 Security Only 4503273 Monthly	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0905						
Service Pack 2	Rollup					
Windows Server 2008 for 32-bit Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0905						
Core installation)						

CVE-2019-0906 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0906 MITRE NVD	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Are Active Directory and Exchange Server affected by this vulnerability? No, Active Directory and Exchange Server are not affected. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0906						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0906						
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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 x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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 Core installation)	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0906						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0906						
Core installation)						
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Important	Remote Code Execution	4499171	Base: 7.8 Temporal: 7 Vector: CVSS: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)	4503263 Security Only 4503285 Monthly Rollup	Important	Remote Code Execution	4499171	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503290 Security Only 4503276 Monthly Rollup	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS: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-	4503276 Monthly Rollup	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7	Yes

CVE-2019-0906						
based systems	4503290 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 Server 2012 R2	4503276 Monthly Rollup 4503290 Security Only	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503291 Security Update	Important	Remote Code Execution	4499154	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0906						
Windows 10 for x64-based Systems	4503291 Security Update	Important	Remote Code Execution	4499154	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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)	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0906						
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Remote Code Execution	4499181	Base: 7.8 Temporal: 7 Vector: CVSS: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 1703 for x64-based Systems	4503279 Security Update	Important	Remote Code Execution	4499181	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7	Yes

CVE-2019-0906						
32-bit Systems					Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7	Yes

CVE-2019-0906						
32-bit Systems					Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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)	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0906						
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0906						
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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-	4503273 Monthly Rollup	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7	Yes

CVE-2019-0906						
based Systems Service Pack 2	4503287 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 Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0907 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0907 MITRE NVD	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** **Are Active Directory and Exchange Server affected by this vulnerability?** No, Active Directory and Exchange Server are not affected.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0907						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0907						
	Rollup					
Windows 7 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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 Core installation)	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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 Itanium-Based Systems	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0907						
Service Pack 1						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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)	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503263 Security Only 4503285 Monthly	Important	Remote Code Execution	4499171	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0907						
	Rollup					
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Important	Remote Code Execution	4499171	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503290 Security Only 4503276 Monthly Rollup	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503276 Monthly Rollup 4503290 Security Only	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503276 Monthly Rollup 4503290	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0907						
	Security Only					
Windows RT 8.1	4503276 Monthly Rollup	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503291 Security Update	Important	Remote Code Execution	4499154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Important	Remote Code Execution	4499154	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7	Yes

CVE-2019-0907						
					Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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)	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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 1703 for 32-bit Systems	4503279 Security Update	Important	Remote Code Execution	4499181	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0907						
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Remote Code Execution	4499181	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 7.8 Temporal: 7 Vector: CVSS: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 32-bit Systems	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7	Yes

CVE-2019-0907						
x64-based Systems					Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7	Yes

CVE-2019-0907						
x64-based Systems					Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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)	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0907						
Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.8 Temporal: 7 Vector: CVSS: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)	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No

CVE-2019-0907						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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-	4503273 Monthly Rollup	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7	Yes

CVE-2019-0907						
based Systems Service Pack 2 (Server Core installation)	4503287 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	

CVE-2019-0908 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0908 MITRE NVD	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** **Are Active Directory and Exchange Server affected by this vulnerability?** No, Active Directory and Exchange Server are not affected. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0908						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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 x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503269 Security Only 4503292	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0908						
Systems Service Pack 1 (Server Core installation)	Monthly Rollup					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0908						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503263 Security Only 4503285 Monthly Rollup	Important	Remote Code Execution	4499171	Base: 7.8 Temporal: 7 Vector: CVSS: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)	4503263 Security Only 4503285 Monthly Rollup	Important	Remote Code Execution	4499171	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0908						
Windows 8.1 for 32-bit systems	4503290 Security Only 4503276 Monthly Rollup	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503276 Monthly Rollup 4503290 Security Only	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503276 Monthly Rollup 4503290 Security Only	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0908						
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503291 Security Update	Important	Remote Code Execution	4499154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Important	Remote Code Execution	4499154	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0908						
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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)	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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 1703 for 32-bit Systems	4503279 Security Update	Important	Remote Code Execution	4499181	Base: 7.8 Temporal: 7 Vector: CVSS: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 1703 for x64-based Systems	4503279 Security Update	Important	Remote Code Execution	4499181	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 7.8 Temporal: 7	Yes

CVE-2019-0908						
32-bit Systems					Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 7.8 Temporal: 7 Vector: CVSS: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 32-bit Systems	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0908						
Core Installation)						
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Remote Code Execution	4499167	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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-	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0908						
based Systems						
Windows Server 2019	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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)	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Important	Remote Code Execution	4497936	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0908						
Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Important	Remote Code Execution	4497936	Base: N/A Temporal: N/A Vector: N/A	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Remote Code Execution	4497936	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Remote Code Execution	4497936	Base: N/A Temporal: N/A Vector: N/A	No
Windows Server 2008 for Itanium-Based Systems	4503287 Security Only 4503273 Monthly	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0908						
Service Pack 2	Rollup					
Windows Server 2008 for 32-bit Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0908						
Core installation)						

CVE-2019-0909 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0909 MITRE NVD	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Are Active Directory and Exchange Server affected by this vulnerability? No, Active Directory and Exchange Server are not affected. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0909						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0909						
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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 x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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 Core installation)	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0909						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0909						
Core installation)						
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Important	Remote Code Execution	4499171	Base: 7.8 Temporal: 7 Vector: CVSS: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)	4503263 Security Only 4503285 Monthly Rollup	Important	Remote Code Execution	4499171	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503290 Security Only 4503276 Monthly Rollup	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS: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-	4503276 Monthly Rollup	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7	Yes

CVE-2019-0909						
based systems	4503290 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 Server 2012 R2	4503276 Monthly Rollup 4503290 Security Only	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503291 Security Update	Important	Remote Code Execution	4499154	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0909						
Windows 10 for x64-based Systems	4503291 Security Update	Important	Remote Code Execution	4499154	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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)	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0909						
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Remote Code Execution	4499181	Base: 7.8 Temporal: 7 Vector: CVSS: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 1703 for x64-based Systems	4503279 Security Update	Important	Remote Code Execution	4499181	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7	Yes

CVE-2019-0909						
32-bit Systems					Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7	Yes

CVE-2019-0909						
32-bit Systems					Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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)	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0909						
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0909						
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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-	4503273 Monthly Rollup	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7	Yes

CVE-2019-0909						
based Systems Service Pack 2	4503287 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 Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0920 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0920 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers. 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 designed to exploit the vulnerability through a Microsoft browser and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the browser 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.	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0920						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	4503273 Monthly Rollup	Moderate	Remote Code Execution	4499149	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4503273 Monthly Rollup 4503259 IE Cumulative	Moderate	Remote Code Execution	4498206	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-2019-0920						
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4503292 Monthly Rollup 4503259 IE Cumulative	Critical	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7 Vector: CVSS: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 7 for x64-based Systems Service Pack 1	4503292 Monthly Rollup 4503259 IE Cumulative	Critical	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503292 Monthly Rollup 4503259 IE	Moderate	Remote Code Execution	4498206	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-2019-0920						
Server 2008 R2 for x64-based Systems Service Pack 1	Cumulative					
Internet Explorer 11 on Windows Server 2012	4503259 IE Cumulative	Moderate	Remote Code Execution	4498206	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 8.1 for 32-bit systems	4503276 Monthly Rollup 4503259 IE Cumulative	Critical	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503276 Monthly Rollup	Critical	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0920						
Windows 8.1 for x64-based systems	4503259 IE Cumulative				Vector: CVSS: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 2012 R2	4503276 Monthly Rollup	Moderate	Remote Code Execution	4499151	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 RT 8.1	4503276 Monthly Rollup	Critical	Remote Code Execution	4499151	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-0920						
Internet Explorer 11 on Windows 10 for x64-based Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2016	4503267 Security Update	Moderate	Remote Code Execution	4494440	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 1607 for 32-bit Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-0920						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 7.5 Temporal: 6.7 Vector: CVSS: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 1703 for 32-bit Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-0920						
10 Version 1703 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for x64-	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-0920						
based Systems						
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-0920						
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-0920						
10 Version 1809 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2019	4503327 Security Update	Moderate	Remote Code Execution	4494441	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-2019-0920						
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No

CVE-2019-0920						
10 Version 1903 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 7.5 Temporal: 6.7 Vector: CVSS: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 10 on Windows Server 2012	4503285 Monthly Rollup 4503259 IE Cumulative	Moderate	Remote Code Execution	4498206	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-2019-0941 - Microsoft IIS Server Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0941 MITRE NVD	**CVE Title:** Microsoft IIS Server Denial of Service Vulnerability **Description:** A denial of service exists in Microsoft IIS Server when the optional request filtering feature improperly handles requests. An attacker who successfully exploited this vulnerability could perform a temporary denial of service against pages configured to use request filtering. To exploit this vulnerability, an attacker could send a specially crafted request to a page utilizing request filtering. The update addresses the vulnerability by changing the way certain requests are processed by the filter. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0941						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Denial of Service	4499164	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-2019-0941						
Windows 7 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Denial of Service	4499164	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 (Server Core installation)	4503269 Security Only 4503292 Monthly Rollup	Important	Denial of Service	4499164	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	4503269 Security Only 4503292 Monthly Rollup	Important	Denial of Service	4499164	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-2019-0941						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Denial of Service	4499164	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Denial of Service	4499149	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	4503263 Security Only 4503285 Monthly Rollup	Important	Denial of Service	4499171	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-2019-0941						
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Important	Denial of Service	4499171	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	4503290 Security Only 4503276 Monthly Rollup	Important	Denial of Service	4499151	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	4503276 Monthly Rollup 4503290 Security Only	Important	Denial of Service	4499151	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	4503276 Monthly Rollup 4503290 Security	Important	Denial of Service	4499151	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-2019-0941						
	Only					
Windows RT 8.1	4503276 Monthly Rollup	Important	Denial of Service	4499151	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 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Denial of Service	4499151	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	4503291 Security Update	Important	Denial of Service	4499154	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Important	Denial of Service	4499154	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	4503267 Security Update	Important	Denial of Service	4494440	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-2019-0941						
Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Important	Denial of Service	4494440	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	4503267 Security Update	Important	Denial of Service	4494440	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)	4503267 Security Update	Important	Denial of Service	4494440	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 1703 for 32-bit Systems	4503279 Security Update	Important	Denial of Service	4499181	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 1703 for x64-based Systems	4503279 Security Update	Important	Denial of Service	4499181	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-2019-0941						
Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Important	Denial of Service	4499179	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	4503284 Security Update	Important	Denial of Service	4499179	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	4503286 Security Update	Important	Denial of Service	4499167	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 x64-based Systems	4503286 Security Update	Important	Denial of Service	4499167	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)	4503286 Security Update	Important	Denial of Service	4499167	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-2019-0941						
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Denial of Service	4499167	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	4503327 Security Update	Important	Denial of Service	4494441	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	4503327 Security Update	Important	Denial of Service	4494441	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 ARM64-based Systems	4503327 Security Update	Important	Denial of Service	4494441	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-2019-0941						
Windows Server 2019	4503327 Security Update	Important	Denial of Service	4494441	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)	4503327 Security Update	Important	Denial of Service	4494441	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 ARM64-based Systems	4503284 Security Update	Important	Denial of Service	4499179	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 32-bit Systems	4503293 Security Update	Important	Denial of Service	4497936	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	4503293 Security Update	Important	Denial of Service	4497936	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	No

CVE-2019-0941						
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Denial of Service	4497936	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)	4503293 Security Update	Important	Denial of Service	4497936	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	No
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Important	Denial of Service	4499149	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems	4503273 Monthly Rollup 4503287 Security	Important	Denial of Service	4499149	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-2019-0941						
Service Pack 2	Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Denial of Service	4499149	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Denial of Service	4499149	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-2019-0943 - Windows ALPC Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0943 MITRE NVD	**CVE Title:** Windows ALPC Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC). An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control over an affected system. The update addresses the vulnerability by correcting how Windows handles calls to ALPC. **FAQ:** None **Mitigations:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0943						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly	Important	Elevation of Privilege	4499164	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0943						
	Rollup					
Windows 7 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0943						
Service Pack 1						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Important	Elevation of Privilege	4499171	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Important	Elevation of Privilege	4499171	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0943						
Windows 8.1 for 32-bit systems	4503290 Security Only 4503276 Monthly Rollup	Important	Elevation of Privilege	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security Only	Important	Elevation of Privilege	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security Only	Important	Elevation of Privilege	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Important	Elevation of Privilege	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0943						
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Elevation of Privilege	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0943						
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0943						
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7	Yes

CVE-2019-0943						
ARM64-based Systems					Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0943						
Windows Server 2019 (Server Core installation)	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0943						
based Systems						
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No

CVE-2019-0948 - Windows Event Viewer Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0948 MITRE NVD	**CVE Title:** Windows Event Viewer Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the Windows Event Viewer (eventvwr.msc) when it improperly parses XML input containing a reference to an	Moderate	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	external entity. An attacker who successfully exploited this vulnerability could read arbitrary files via an XML external entity (XXE) declaration. To exploit the vulnerability, an attacker could create a file containing specially crafted XML content and convince an authenticated user to import the file. The update addresses the vulnerability by modifying the way that the Event Viewer parses XML input. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is unauthorized file system access - reading from file system. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00		

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

Affected Software

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

CVE-2019-0948						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Moderate	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0948						
Windows 7 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Moderate	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/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)	4503269 Security Only 4503292 Monthly Rollup	Moderate	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-	4503269 Security Only	Moderate	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-0948						
Based Systems Service Pack 1	4503292 Monthly Rollup				CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Moderate	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Moderate	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0948						
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Moderate	Information Disclosure	4499171	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Moderate	Information Disclosure	4499171	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4503290 Security Only 4503276 Monthly	Moderate	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0948						
	Rollup					
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security Only	Moderate	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security Only	Moderate	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Moderate	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0948						
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Moderate	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4503291 Security Update	Moderate	Information Disclosure	4499154	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Moderate	Information Disclosure	4499154	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4503267 Security Update	Moderate	Information Disclosure	4494440	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0948						
Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Moderate	Information Disclosure	4494440	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Moderate	Information Disclosure	4494440	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4503267 Security Update	Moderate	Information Disclosure	4494440	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Moderate	Information Disclosure	4499181	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0948						
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Moderate	Information Disclosure	4499181	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Moderate	Information Disclosure	4499179	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Moderate	Information Disclosure	4499179	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Moderate	Information Disclosure	4499167	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for	4503286 Security	Moderate	Information Disclosure	4499167	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-0948						
x64-based Systems	Update				CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4503286 Security Update	Moderate	Information Disclosure	4499167	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Moderate	Information Disclosure	4499167	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Moderate	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0948						
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Moderate	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Moderate	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4503327 Security Update	Moderate	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4503327 Security Update	Moderate	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0948						
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Moderate	Information Disclosure	4499179	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Moderate	Information Disclosure	4497936	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Moderate	Information Disclosure	4497936	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Moderate	Information Disclosure	4497936	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0948						
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Moderate	Information Disclosure	4497936	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	No
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Moderate	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security	Moderate	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0948						
	Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Moderate	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/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)	4503273 Monthly Rollup 4503287 Security Only	Moderate	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0959 - Windows Common Log File System Driver Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0959 MITRE NVD	**CVE Title:** Windows Common Log File System Driver Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run processes in an elevated context. To exploit the vulnerability, an attacker would first have to log on to the system, and then run a specially crafted application to take control over the affected system. The security update addresses the vulnerability by correcting how CLFS handles objects in memory. **FAQ:** None **Mitigations:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0959						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0959						
Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0959						
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7 Temporal: 6.3	Yes

CVE-2019-0959						
32-bit Systems					Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No

CVE-2019-0960 - Win32k Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0960 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. 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:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0960						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0960						
Windows 7 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0960						
Service Pack 1						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems	4503287 Security Only 4503273 Monthly	Important	Elevation of Privilege	4499149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0960						
Service Pack 2	Rollup					
Windows Server 2008 for 32-bit Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0960						
Core installation)						

CVE-2019-0968 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0968 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.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0968						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based	4503269 Security Only	Important	Information Disclosure	4499164	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-0968						
Systems Service Pack 1 (Server Core installation)	4503292 Monthly Rollup				CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0968						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Important	Information Disclosure	4499149	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit	4503273 Monthly Rollup	Important	Information Disclosure	4499149	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-0968						
Systems Service Pack 2	4503287 Security Only				CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0972 - Local Security Authority Subsystem Service Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0972 MITRE NVD	**CVE Title:** Local Security Authority Subsystem Service Denial of Service Vulnerability **Description:** This security update corrects a denial of service in the Local Security Authority Subsystem Service (LSASS) caused when an authenticated attacker sends a specially crafted authentication request. A remote attacker who successfully exploited this vulnerability could cause a denial of service on the target system's LSASS service, which triggers an automatic reboot of the system. The security update addresses the vulnerability by changing the way that LSASS handles specially crafted authentication requests. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0972						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Denial of Service	4499164	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes

CVE-2019-0972						
Windows 7 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Denial of Service	4499164	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4503269 Security Only 4503292 Monthly Rollup	Important	Denial of Service	4499164	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Denial of Service	4499164	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes

CVE-2019-0972						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Denial of Service	4499164	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Denial of Service	4499149	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Important	Denial of Service	4499171	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes

CVE-2019-0972						
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Important	Denial of Service	4499171	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows 8.1 for 32-bit systems	4503290 Security Only 4503276 Monthly Rollup	Important	Denial of Service	4499151	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security Only	Important	Denial of Service	4499151	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security	Important	Denial of Service	4499151	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes

CVE-2019-0972						
	Only					
Windows RT 8.1	4503276 Monthly Rollup	Important	Denial of Service	4499151	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Denial of Service	4499151	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows 10 for 32-bit Systems	4503291 Security Update	Important	Denial of Service	4499154	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Important	Denial of Service	4499154	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows Server 2016	4503267 Security Update	Important	Denial of Service	4494440	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes

CVE-2019-0972						
Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Important	Denial of Service	4494440	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Important	Denial of Service	4494440	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows Server 2016 (Server Core installation)	4503267 Security Update	Important	Denial of Service	4494440	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Denial of Service	4499181	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Denial of Service	4499181	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes

CVE-2019-0972						
Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Important	Denial of Service	4499179	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Denial of Service	4499179	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Important	Denial of Service	4499167	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Denial of Service	4499167	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows Server, version 1803 (Server Core Installation)	4503286 Security Update	Important	Denial of Service	4499167	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes

CVE-2019-0972						
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Denial of Service	4499167	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Denial of Service	4494441	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Denial of Service	4494441	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Important	Denial of Service	4494441	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows Server 2019	4503327 Security Update	Important	Denial of Service	4494441	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes

CVE-2019-0972						
Windows Server 2019 (Server Core installation)	4503327 Security Update	Important	Denial of Service	4494441	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Important	Denial of Service	4499179	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Important	Denial of Service	4497936	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Important	Denial of Service	4497936	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Denial of Service	4497936	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes

CVE-2019-0972						
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Denial of Service	4497936	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	No
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Important	Denial of Service	4499149	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Denial of Service	4499149	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes
Windows Server 2008 for x64-based Systems	4503273 Monthly Rollup 4503287 Security	Important	Denial of Service	4499149	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes

CVE-2019-0972						
Service Pack 2	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Denial of Service	4499149	Base: 6.5 Temporal: 5.6 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	Yes

CVE-2019-0973 - Windows Installer Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0973 MITRE NVD	**CVE Title:** Windows Installer Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	A locally authenticated attacker could run arbitrary code with elevated system privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by correcting the input sanitization error to preclude unintended elevation. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0973						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0973						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0973						
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Important	Elevation of Privilege	4499171	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Important	Elevation of Privilege	4499171	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4503290 Security Only 4503276 Monthly Rollup	Important	Elevation of Privilege	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security	Important	Elevation of Privilege	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0973						
	Only					
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security Only	Important	Elevation of Privilege	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Important	Elevation of Privilege	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Elevation of Privilege	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0973						
Windows 10 for x64-based Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0973						
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0973						
Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0973						
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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-	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0973						
based Systems						
Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No

CVE-2019-0973						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Important	Elevation of Privilege	4499149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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-	4503273 Monthly Rollup	Important	Elevation of Privilege	4499149	Base: 7.8 Temporal: 7	Yes

CVE-2019-0973						
based Systems Service Pack 2 (Server Core installation)	4503287 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	

CVE-2019-0974 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0974 MITRE NVD	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** **Are Active Directory and Exchange Server affected by this vulnerability?** No, Active Directory and Exchange Server are not affected. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0974						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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 x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0974						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0974						
(Server Core installation)						
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Important	Remote Code Execution	4499171	Base: 7.8 Temporal: 7 Vector: CVSS: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)	4503263 Security Only 4503285 Monthly Rollup	Important	Remote Code Execution	4499171	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503290 Security Only 4503276 Monthly Rollup	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0974						
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security Only	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503276 Monthly Rollup 4503290 Security Only	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Remote Code Execution	4499151	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0974						
Windows 10 for 32-bit Systems	4503291 Security Update	Important	Remote Code Execution	4499154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Important	Remote Code Execution	4499154	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0974						
Windows Server 2016 (Server Core installation)	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.8 Temporal: 7 Vector: CVSS: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 1703 for 32-bit Systems	4503279 Security Update	Important	Remote Code Execution	4499181	Base: 7.8 Temporal: 7 Vector: CVSS: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 1703 for x64-based Systems	4503279 Security Update	Important	Remote Code Execution	4499181	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 7.8 Temporal: 7	Yes

CVE-2019-0974						
x64-based Systems					Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7 Vector: CVSS: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-	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0974						
based Systems						
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0974						
Windows Server 2019 (Server Core installation)	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No

CVE-2019-0974						
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.8 Temporal: 7 Vector: CVSS: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)	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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	4503273 Monthly Rollup	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7	Yes

CVE-2019-0974						
Systems Service Pack 2	4503287 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 Server 2008 for x64-based Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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)	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0977 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0977 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.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0977						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0977						
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0977						
(Server Core installation)	Rollup					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for	4503273 Monthly	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-0977						
32-bit Systems Service Pack 2 (Server Core installation)	Rollup 4503287 Security Only				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503273 Monthly Rollup 4503287 Security	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0977						
	Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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)	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0983 - Windows Storage Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0983 MITRE NVD	**CVE Title:** Windows Storage Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations. An attacker who successfully exploited this vulnerability could gain elevated privileges on the victim system. To exploit the vulnerability, an attacker would first have to gain execution on the victim system, then run a specially crafted application. The security update addresses the vulnerability by correcting how the Storage Services handles file operations. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0983						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2016	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0983						
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0983						
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7	Yes

CVE-2019-0983						
ARM64-based Systems					Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0983						
Windows Server 2019 (Server Core installation)	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0983						
based Systems						
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No

CVE-2019-0984 - Windows Common Log File System Driver Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0984 MITRE NVD	**CVE Title:** Windows Common Log File System Driver 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 Common Log File System (CLFS) driver improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run processes in an elevated context. To exploit the vulnerability, an attacker would first have to log on to the system, and then run a specially crafted application to take control over the affected system. The security update addresses the vulnerability by correcting how CLFS handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0984						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based	4503269 Security Only 4503292	Important	Elevation of Privilege	4499164	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0984						
Systems Service Pack 1 (Server Core installation)	Monthly Rollup					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit	4503273 Monthly Rollup	Important	Elevation of Privilege	4499149	Base: 7 Temporal: 6.3	Yes

CVE-2019-0984						
Systems Service Pack 2 (Server Core installation)	4503287 Security Only				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Important	Elevation of Privilege	4499171	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Important	Elevation of Privilege	4499171	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4503290 Security Only 4503276 Monthly Rollup	Important	Elevation of Privilege	4499151	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0984						
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security Only	Important	Elevation of Privilege	4499151	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security Only	Important	Elevation of Privilege	4499151	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Important	Elevation of Privilege	4499151	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Elevation of Privilege	4499151	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0984						
Windows 10 for 32-bit Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0984						
Windows Server 2016 (Server Core installation)	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0984						
x64-based Systems						
Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0984						
based Systems						
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0984						
Windows Server 2019 (Server Core installation)	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7 Temporal: 6.3	Yes

CVE-2019-0984						
ARM64-based Systems					Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Important	Elevation of Privilege	4499149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0984						
Windows Server 2008 for x64-based Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0985 - Microsoft Speech API Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0985 MITRE NVD	**CVE Title:** Microsoft Speech API Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Microsoft Speech API (SAPI) improperly handles text-to-speech (TTS) input. The vulnerability could corrupt memory in a way that enables an attacker to execute arbitrary code in the context of the current user. To exploit the vulnerability, an attacker would need to convince a user to open a specially crafted document containing TTS content invoked through a scripting language. The update address the vulnerability by modifying how the system handles objects in memory. **FAQ:** None	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0985						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems	4503269 Security Only 4503292	Critical	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0985						
Service Pack 1	Monthly Rollup					
Windows 7 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Critical	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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 Core installation)	4503269 Security Only 4503292 Monthly Rollup	Critical	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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 Itanium-Based Systems	4503269 Security Only 4503292 Monthly Rollup	Critical	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0985						
Service Pack 1						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Critical	Remote Code Execution	4499164	Base: 7.8 Temporal: 7 Vector: CVSS: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-2019-0986 - Windows User Profile Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0986 MITRE NVD	**CVE Title:** Windows User Profile 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 User Profile Service (ProfSvc) improperly handles symlinks. An attacker who successfully exploited this vulnerability could delete files and folders in an elevated context. 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 delete files or folders of their choosing. The security update addresses the vulnerability by correcting how the Windows User Profile Service handles symlinks. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0986						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based	4503269 Security Only 4503292	Important	Elevation of Privilege	4499164	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0986						
Systems Service Pack 1 (Server Core installation)	Monthly Rollup					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0986						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Important	Elevation of Privilege	4499171	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Important	Elevation of Privilege	4499171	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0986						
Windows 8.1 for 32-bit systems	4503290 Security Only 4503276 Monthly Rollup	Important	Elevation of Privilege	4499151	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security Only	Important	Elevation of Privilege	4499151	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security Only	Important	Elevation of Privilege	4499151	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Important	Elevation of Privilege	4499151	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0986						
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Elevation of Privilege	4499151	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0986						
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 6.3 Temporal: 5.7	Yes

CVE-2019-0986						
32-bit Systems					Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0986						
Core Installation)						
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0986						
based Systems						
Windows Server 2019	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0986						
Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	No
Windows Server 2008 for Itanium-Based Systems	4503287 Security Only 4503273 Monthly	Important	Elevation of Privilege	4499149	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0986						
Service Pack 2	Rollup					
Windows Server 2008 for 32-bit Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0986						
Core installation)						

CVE-2019-0988 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0988 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0988						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4503292 Monthly Rollup 4503259 IE Cumulative	Critical	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7 Vector: CVSS: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 7 for x64-based	4503292 Monthly Rollup 4503259 IE Cumulative	Critical	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-0988						
Systems Service Pack 1						
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503292 Monthly Rollup 4503259 IE Cumulative	Moderate	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012	4503259 IE Cumulative	Moderate	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503276 Monthly Rollup	Critical	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0988						
Windows 8.1 for 32-bit systems	4503259 IE Cumulative				Vector: CVSS: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 x64-based systems	4503276 Monthly Rollup 4503259 IE Cumulative	Critical	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4503276 Monthly Rollup	Moderate	Remote Code Execution	4499151	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows RT 8.1	4503276 Monthly Rollup	Critical	Remote Code Execution	4499151	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-0988						
Internet Explorer 11 on Windows 10 for 32-bit Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2016	4503267 Security Update	Moderate	Remote Code Execution	4494440	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-0988						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 7.5 Temporal: 6.7 Vector: CVSS: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 x64-based Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-0988						
10 Version 1703 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-0988						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-0988						
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0988						
Windows 10 Version 1809 for 32-bit Systems					Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-0988						
ARM64-based Systems						
Internet Explorer 11 on Windows Server 2019	4503327 Security Update	Moderate	Remote Code Execution	4494441	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-0988						
10 Version 1903 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-0988						
based Systems						
Internet Explorer 10 on Windows Server 2012	4503285 Monthly Rollup 4503259 IE Cumulative	Moderate	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-0989 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0989 MITRE NVD	**CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current	Critical	Remote Code Execution

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0989						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0989						
10 for x64-based Systems					Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows Server 2016	4503267 Security Update	Moderate	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0989						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0989						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0989						
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0989						
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2019	4503327 Security Update	Moderate	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0989						
10 Version 1903 for 32-bit Systems					Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	No
Microsoft Edge on Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore on ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4497936	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0990 - Scripting Engine Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0990 MITRE NVD	**CVE Title:** Scripting Engine Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. In a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site. The security update addresses the vulnerability by changing how the scripting engine handles objects in memory. **FAQ:**	Critical	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 uninitialized memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0990						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4503291 Security Update	Critical	Information Disclosure	4499154	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4503291 Security Update	Critical	Information Disclosure	4499154	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2016	4503267 Security Update	Moderate	Information Disclosure	4494440	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4503267 Security Update	Critical	Information Disclosure	4494440	Base: 6.5 Temporal: 5.9 Vector:	Yes

CVE-2019-0990						
1607 for 32-bit Systems					CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Critical	Information Disclosure	4494440	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Critical	Information Disclosure	4499181	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for	4503279 Security Update	Critical	Information Disclosure	4499181	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0990						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Critical	Information Disclosure	4499179	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Critical	Information Disclosure	4499179	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Critical	Information Disclosure	4499167	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0990						
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Critical	Information Disclosure	4499167	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Critical	Information Disclosure	4499167	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Critical	Information Disclosure	4494441	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0990						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Critical	Information Disclosure	4494441	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Critical	Information Disclosure	4494441	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2019	4503327 Security Update	Moderate	Information Disclosure	4494441	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4503284 Security	Critical	Information Disclosure	4499179	Base: 6.5 Temporal: 5.9 Vector:	Yes

CVE-2019-0990						
10 Version 1709 for ARM64-based Systems	Update				CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Critical	Information Disclosure	4497936	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Critical	Information Disclosure	4497936	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	No
Microsoft Edge on Windows 10 Version	4503293 Security Update	Critical	Information Disclosure	4497936	Base: 6.5 Temporal: 5.9 Vector:	Yes

CVE-2019-0990						
1903 for ARM64-based Systems					CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
ChakraCore on ChakraCore	Release Notes Security Update	Critical	Information Disclosure	4497936	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-0991 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0991	**CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory	Critical	Remote Code Execution

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0991						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0991						
10 for x64-based Systems					Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows Server 2016	4503267 Security Update	Moderate	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0991						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0991						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0991						
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0991						
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2019	4503327 Security Update	Moderate	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0991						
10 Version 1903 for 32-bit Systems					Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	No
Microsoft Edge on Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore on ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-0992 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0992 MITRE NVD	**CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0992						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2016	4503267 Security Update	Moderate	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0992						
1607 for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0992						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0992						
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0992						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2019	4503327 Security Update	Moderate	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0992						
10 Version 1709 for ARM64-based Systems					Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	No
Microsoft Edge on Windows 10 Version	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0992						
1903 for ARM64-based Systems						

CVE-2019-0993 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0993 MITRE NVD	**CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0993						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2016	4503267 Security Update	Moderate	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0993						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0993						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0993						
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0993						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0993						
Microsoft Edge on Windows Server 2019	4503327 Security Update	Moderate	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	No

CVE-2019-0993						
1903 for x64-based Systems						
Microsoft Edge on Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore on ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-0996 - Azure DevOps Server Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0996 MITRE NVD	**CVE Title:** Azure DevOps Server Spoofing Vulnerability **Description:** A spoofing vulnerability exists in Azure DevOps Server when it improperly handles requests to authorize applications, resulting in a cross-site request forgery. An attacker who successfully exploited this vulnerability could bypass OAuth protections and register an application on behalf of the targeted user. To exploit this vulnerability, an attacker would need to create a page specifically designed to cause a cross-site request. The attacker would then need to convince a targeted user to click a link to the malicious page. The update addresses the vulnerability by modifying how Azure DevOps Server protects application registration requests. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0996						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Azure DevOps Server 2019	Release Notes Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0998 - Windows Storage Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0998 MITRE NVD	**CVE Title:** Windows Storage Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations. An attacker who successfully exploited this vulnerability could gain elevated privileges on the victim system. To exploit the vulnerability, an attacker would first have to gain execution on the victim system, then run a specially crafted application. The security update addresses the vulnerability by correcting how the Storage Services handles file operations. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0998						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0998						
x64-based Systems						
Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0998						
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0998						
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0998						
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No

CVE-2019-1002 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1002 MITRE NVD	**CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1002						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4503267 Security Update	Moderate	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1002						
Server 2016						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1002						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1002						
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1002						
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1003 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1003 MITRE NVD	**CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current	Critical	Remote Code Execution

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1003						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-1003						
10 for x64-based Systems					Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows Server 2016	4503267 Security Update	Moderate	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1003						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1003						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1003						
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1003						
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2019	4503327 Security Update	Moderate	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-1003						
10 Version 1903 for 32-bit Systems					Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	No
Microsoft Edge on Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore on ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-1005 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1005 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers. 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 designed to exploit the vulnerability through a Microsoft browser and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the browser 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.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** **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 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1005						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	4503273 Monthly Rollup 4503259 IE Cumulative	Low	Remote Code Execution	4498206	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	4503273 Monthly Rollup 4503259 IE Cumulative	Low	Remote Code Execution	4498206	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-2019-1005						
x64-based Systems Service Pack 2						
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4503292 Monthly Rollup 4503259 IE Cumulative	Important	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	Yes
Internet Explorer 11 on Windows 7 for x64-based Systems	4503292 Monthly Rollup 4503259 IE Cumulative	Important	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	Yes

CVE-2019-1005						
Service Pack 1						
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503292 Monthly Rollup 4503259 IE Cumulative	Low	Remote Code Execution	4498206	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	4503259 IE Cumulative	Low	Remote Code Execution	4498206	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	4503276 Monthly Rollup 4503259 IE	Important	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	Yes

CVE-2019-1005						
8.1 for 32-bit systems	Cumulative					
Internet Explorer 11 on Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503259 IE Cumulative	Important	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	Yes
Internet Explorer 11 on Windows Server 2012 R2	4503276 Monthly Rollup	Low	Remote Code Execution	4499151	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 RT 8.1	4503276 Monthly Rollup	Important	Remote Code Execution	4499151	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	Yes

CVE-2019-1005						
Internet Explorer 11 on Windows 10 for 32-bit Systems	4503291 Security Update	Important	Remote Code Execution	4499154	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4503291 Security Update	Important	Remote Code Execution	4499154	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	Yes
Internet Explorer 11 on Windows Server 2016	4503267 Security Update	Low	Remote Code Execution	4494440	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-2019-1005						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	Yes
Internet Explorer 11 on Windows	4503279 Security Update	Important	Remote Code Execution	4499181	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	Yes

CVE-2019-1005						
10 Version 1703 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Remote Code Execution	4499181	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 Version 1709 for	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	Yes

CVE-2019-1005						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	Yes

CVE-2019-1005						
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	Yes
Internet Explorer 11 on	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-1005						
Windows 10 Version 1809 for 32-bit Systems					Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 Version 1809 for	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	Yes

CVE-2019-1005						
ARM64-based Systems						
Internet Explorer 11 on Windows Server 2019	4503327 Security Update	Low	Remote Code Execution	4494441	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 ARM64-based Systems	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	Yes
Internet Explorer 11 on Windows	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	Yes

CVE-2019-1005						
10 Version 1903 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	No
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	Yes

CVE-2019-1005						
based Systems						
Internet Explorer 10 on Windows Server 2012	4503285 Monthly Rollup 4503259 IE Cumulative	Low	Remote Code Execution	4498206	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-2019-1007 - Windows Audio Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1007 MITRE NVD	**CVE Title:** Windows Audio Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege exists in Windows Audio Service. An attacker who successfully exploited the vulnerability could run arbitrary code with elevated privileges.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, an attacker could run a specially crafted application that could exploit the vulnerability. This vulnerability by itself does not allow arbitrary code to be run. However, this vulnerability could be used in conjunction with one or more vulnerabilities (e.g. a remote code execution vulnerability and another elevation of privilege) that could take advantage of the elevated privileges when running. The update addresses the vulnerability by correcting how the Windows Audio Service handles processes these requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1007						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1007						
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1007						
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7	Yes

CVE-2019-1007						
ARM64-based Systems					Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1007						
Windows Server 2019 (Server Core installation)	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1007						
based Systems						
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No

CVE-2019-1009 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1009 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 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1009						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1009						
	Rollup					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for	4503269 Security	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-1009						
x64-based Systems Service Pack 1	Only 4503292 Monthly Rollup				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503287 Security Only 4503273 Monthly	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1009						
Service Pack 2	Rollup					
Windows Server 2008 for 32-bit Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503273 Monthly Rollup 450328	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1009						
Service Pack 2 (Server Core installation)	7 Security Only					

CVE-2019-1010 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1010 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 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1010						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1010						
	Rollup					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-1010						
Systems Service Pack 1	4503292 Monthly Rollup				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Important	Information Disclosure	4499171	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1010						
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Important	Information Disclosure	4499171	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503290 Security Only 4503276 Monthly Rollup	Important	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503276 Monthly Rollup 4503290 Security	Important	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1010						
	Only					
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security Only	Important	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Important	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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)	4503276 Monthly Rollup 4503290 Security Only	Important	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1010						
Windows 10 for 32-bit Systems	4503291 Security Update	Important	Information Disclosure	4499154	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503291 Security Update	Important	Information Disclosure	4499154	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4503267 Security Update	Important	Information Disclosure	4494440	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503267 Security Update	Important	Information Disclosure	4494440	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for	4503267 Security	Important	Information Disclosure	4494440	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-1010						
x64-based Systems	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2016 (Server Core installation)	4503267 Security Update	Important	Information Disclosure	4494440	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Information Disclosure	4499181	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Information Disclosure	4499181	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503284 Security Update	Important	Information Disclosure	4499179	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1010						
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Information Disclosure	4499179	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503286 Security Update	Important	Information Disclosure	4499167	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503286 Security Update	Important	Information Disclosure	4499167	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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)	4503286 Security Update	Important	Information Disclosure	4499167	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1010						
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Information Disclosure	4499167	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1010						
Windows Server 2019	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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)	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503284 Security Update	Important	Information Disclosure	4499179	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503293 Security Update	Important	Information Disclosure	4497936	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1010						
Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Important	Information Disclosure	4497936	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Information Disclosure	4497936	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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)	4503293 Security Update	Important	Information Disclosure	4497936	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	No
Windows Server 2008 for Itanium-Based	4503287 Security Only 450327	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1010						
Systems Service Pack 2	3 Monthly Rollup					
Windows Server 2008 for 32-bit Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503273 Monthly Rollup	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-1010						
Systems Service Pack 2 (Server Core installation)	4503287 Security Only				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	

CVE-2019-1011 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1011 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 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1011						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1011						
	Rollup					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for	4503269 Security	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-1011						
x64-based Systems Service Pack 1	Only 4503292 Monthly Rollup				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503287 Security Only 4503273 Monthly	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1011						
Service Pack 2	Rollup					
Windows Server 2008 for 32-bit Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503273 Monthly Rollup 450328	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1011						
Service Pack 2 (Server Core installation)	7 Security Only					

CVE-2019-1012 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1012 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 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1012						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1012						
	Rollup					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-1012						
Systems Service Pack 1	4503292 Monthly Rollup				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Important	Information Disclosure	4499171	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1012						
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Important	Information Disclosure	4499171	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503290 Security Only 4503276 Monthly Rollup	Important	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503276 Monthly Rollup 4503290 Security	Important	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1012						
	Only					
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security Only	Important	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Important	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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)	4503276 Monthly Rollup 4503290 Security Only	Important	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1012						
Windows 10 for 32-bit Systems	4503291 Security Update	Important	Information Disclosure	4499154	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503291 Security Update	Important	Information Disclosure	4499154	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4503267 Security Update	Important	Information Disclosure	4494440	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503267 Security Update	Important	Information Disclosure	4494440	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for	4503267 Security	Important	Information Disclosure	4494440	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-1012						
x64-based Systems	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2016 (Server Core installation)	4503267 Security Update	Important	Information Disclosure	4494440	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Information Disclosure	4499181	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Information Disclosure	4499181	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503284 Security Update	Important	Information Disclosure	4499179	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1012						
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Information Disclosure	4499179	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503286 Security Update	Important	Information Disclosure	4499167	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503286 Security Update	Important	Information Disclosure	4499167	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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)	4503286 Security Update	Important	Information Disclosure	4499167	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1012						
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Information Disclosure	4499167	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1012						
Windows Server 2019	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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)	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503284 Security Update	Important	Information Disclosure	4499179	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503293 Security Update	Important	Information Disclosure	4497936	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1012						
Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Important	Information Disclosure	4497936	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Information Disclosure	4497936	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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)	4503293 Security Update	Important	Information Disclosure	4497936	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	No
Windows Server 2008 for Itanium-Based	4503287 Security Only 450327	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1012						
Systems Service Pack 2	3 Monthly Rollup					
Windows Server 2008 for 32-bit Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503273 Monthly Rollup	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-1012						
Systems Service Pack 2 (Server Core installation)	4503287 Security Only				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	

CVE-2019-1013 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1013 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 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1013						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1013						
	Rollup					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for	4503269 Security	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-1013						
x64-based Systems Service Pack 1	Only 4503292 Monthly Rollup				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503287 Security Only 4503273 Monthly	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1013						
Service Pack 2	Rollup					
Windows Server 2008 for 32-bit Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503273 Monthly Rollup 450328	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1013						
Service Pack 2 (Server Core installation)	7 Security Only					

CVE-2019-1014 - Win32k Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1014 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 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1014						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1014						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1014						
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Important	Elevation of Privilege	4499171	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Important	Elevation of Privilege	4499171	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4503290 Security Only 4503276 Monthly Rollup	Important	Elevation of Privilege	4499151	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security	Important	Elevation of Privilege	4499151	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1014						
	Only					
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security Only	Important	Elevation of Privilege	4499151	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Important	Elevation of Privilege	4499151	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Elevation of Privilege	4499151	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1014						
Windows 10 for x64-based Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1014						
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7 Temporal: 6.3	Yes

CVE-2019-1014						
32-bit Systems					Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1014						
32-bit Systems						
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1014						
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1014						
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Important	Elevation of Privilege	4499149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based	4503273 Monthly Rollup 4503287	Important	Elevation of Privilege	4499149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1014						
Systems Service Pack 2	Security Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1015 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1015	**CVE Title:** Windows GDI Information Disclosure Vulnerability **Description:**	Important	Information Disclosure

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1015						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1015						
	Monthly Rollup					
Windows 7 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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)	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1015						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503273 Monthly Rollup 4503287 Security	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1015						
(Server Core installation)	Only					
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Important	Information Disclosure	4499171	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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)	4503263 Security Only 4503285 Monthly Rollup	Important	Information Disclosure	4499171	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for	4503287 Security	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-1015						
Itanium-Based Systems Service Pack 2	Only 4503273 Monthly Rollup				CVSS:3.0/AV:L/AC:H/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	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1015						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1016 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1016	**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	Important	Information Disclosure

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1016						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1016						
	Rollup					
Windows 7 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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)	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for	4503269 Security	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-1016						
Itanium-Based Systems Service Pack 1	Only 4503292 Monthly Rollup				CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1016						
installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503273 Monthly Rollup 450328	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1016						
Service Pack 2	7 Security Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1017 - Win32k Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1017 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. 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:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1017						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1017						
Windows 7 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1017						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Important	Elevation of Privilege	4499171	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1017						
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Important	Elevation of Privilege	4499171	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4503290 Security Only 4503276 Monthly Rollup	Important	Elevation of Privilege	4499151	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security Only	Important	Elevation of Privilege	4499151	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security	Important	Elevation of Privilege	4499151	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1017						
	Only					
Windows RT 8.1	4503276 Monthly Rollup	Important	Elevation of Privilege	4499151	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Elevation of Privilege	4499151	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1017						
Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1017						
x64-based Systems						
Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1017						
Windows Server, version 1803 (Server Core Installation)	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1017						
Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7 Temporal: 6.3	Yes

CVE-2019-1017						
32-bit Systems					Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows Server 2008 for Itanium-Based	4503287 Security Only 4503273	Important	Elevation of Privilege	4499149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1017						
Systems Service Pack 2	Monthly Rollup					
Windows Server 2008 for 32-bit Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1017						
Core installation)						

CVE-2019-1018 - DirectX Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1018 MITRE NVD	**CVE Title:** DirectX Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses the vulnerability by correcting how DirectX handles objects in memory.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1018						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-1018						
Windows 10 for 32-bit Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1018						
Windows Server 2016 (Server Core installation)	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7 Temporal: 6.3	Yes

CVE-2019-1018						
x64-based Systems					Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1018						
based Systems						
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1018						
Windows Server 2019 (Server Core installation)	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1019 - Microsoft Windows Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1019	**CVE Title:** Microsoft Windows Security Feature Bypass Vulnerability **Description:**	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A security feature bypass vulnerability exists where a NETLOGON message is able to obtain the session key and sign messages. To exploit this vulnerability, an attacker could send a specially crafted authentication request. An attacker who successfully exploited this vulnerability could access another machine using the original user privileges. The issue has been addressed by changing how NTLM validates network authentication messages. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1019						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Security Feature Bypass	4499164	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Security Feature Bypass	4499164	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based	4503269 Security Only 4503292	Important	Security Feature Bypass	4499164	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1019						
Systems Service Pack 1 (Server Core installation)	Monthly Rollup					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Security Feature Bypass	4499164	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Security Feature Bypass	4499164	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit	4503273 Monthly Rollup	Important	Security Feature Bypass	4499149	Base: 8.5 Temporal: 7.6	Yes

CVE-2019-1019						
Systems Service Pack 2 (Server Core installation)	4503287 Security Only				Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Important	Security Feature Bypass	4499171	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Important	Security Feature Bypass	4499171	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4503290 Security Only 4503276 Monthly Rollup	Important	Security Feature Bypass	4499151	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1019						
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security Only	Important	Security Feature Bypass	4499151	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security Only	Important	Security Feature Bypass	4499151	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Important	Security Feature Bypass	4499151	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Security Feature Bypass	4499151	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1019						
Windows 10 for 32-bit Systems	4503291 Security Update	Important	Security Feature Bypass	4499154	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Important	Security Feature Bypass	4499154	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4503267 Security Update	Important	Security Feature Bypass	4494440	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Important	Security Feature Bypass	4494440	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Important	Security Feature Bypass	4494440	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1019						
Windows Server 2016 (Server Core installation)	4503267 Security Update	Important	Security Feature Bypass	4494440	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Security Feature Bypass	4499181	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Security Feature Bypass	4499181	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Important	Security Feature Bypass	4499179	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Security Feature Bypass	4499179	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1019						
Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Important	Security Feature Bypass	4499167	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Security Feature Bypass	4499167	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4503286 Security Update	Important	Security Feature Bypass	4499167	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Security Feature Bypass	4499167	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1019						
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Security Feature Bypass	4494441	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Security Feature Bypass	4494441	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Important	Security Feature Bypass	4494441	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4503327 Security Update	Important	Security Feature Bypass	4494441	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4503327 Security Update	Important	Security Feature Bypass	4494441	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1019						
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Important	Security Feature Bypass	4499179	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Important	Security Feature Bypass	4497936	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Important	Security Feature Bypass	4497936	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Security Feature Bypass	4497936	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1019						
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Security Feature Bypass	4497936	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Important	Security Feature Bypass	4499149	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Security Feature Bypass	4499149	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based	4503273 Monthly Rollup 4503287	Important	Security Feature Bypass	4499149	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1019						
Systems Service Pack 2	Security Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Security Feature Bypass	4499149	Base: 8.5 Temporal: 7.6 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1021 - Windows Audio Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1021 MITRE NVD	**CVE Title:** Windows Audio Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege exists in Windows Audio Service. An attacker who successfully exploited the vulnerability could run arbitrary code with elevated privileges. To exploit the vulnerability, an attacker could run a specially crafted application that could exploit the vulnerability. This vulnerability by itself does not allow arbitrary code to be run. However, this vulnerability could be used in conjunction with one or more vulnerabilities (e.g. a remote code execution vulnerability and another elevation of privilege) that could take advantage of the elevated privileges when running. The update addresses the vulnerability by correcting how the Windows Audio Service handles processes these requests. **FAQ:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1021						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1021						
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1021						
Windows Server, version 1803 (Server Core Installation)	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1021						
Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7	Yes

CVE-2019-1021						
1903 for 32-bit Systems					Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No

CVE-2019-1022 - Windows Audio Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1022 MITRE NVD	**CVE Title:** Windows Audio Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege exists in Windows Audio Service. An attacker who successfully exploited the vulnerability could run arbitrary code with elevated privileges. To exploit the vulnerability, an attacker could run a specially crafted application that could exploit the vulnerability. This vulnerability by itself does not allow arbitrary code to be run. However, this vulnerability could be used in conjunction with one or more vulnerabilities (e.g. a remote code execution vulnerability and another elevation of privilege) that could take advantage of the elevated privileges when running. The update addresses the vulnerability by correcting how the Windows Audio Service handles processes these requests. **FAQ:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1022						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1022						
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1022						
Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No

CVE-2019-1023 - Scripting Engine Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1023 MITRE NVD	**CVE Title:** Scripting Engine Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. In a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site. The security update addresses the vulnerability by changing how the scripting engine handles objects in memory. **FAQ:**	Critical	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 uninitialized memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1023						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4503291 Security Update	Critical	Information Disclosure	4499154	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4503291 Security Update	Critical	Information Disclosure	4499154	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2016	4503267 Security Update	Moderate	Information Disclosure	4494440	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4503267 Security Update	Critical	Information Disclosure	4494440	Base: 6.5 Temporal: 5.9 Vector:	Yes

CVE-2019-1023						
1607 for 32-bit Systems					CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Critical	Information Disclosure	4494440	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Critical	Information Disclosure	4499181	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for	4503279 Security Update	Critical	Information Disclosure	4499181	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1023						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Critical	Information Disclosure	4499179	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Critical	Information Disclosure	4499179	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Critical	Information Disclosure	4499167	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1023						
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Critical	Information Disclosure	4499167	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Critical	Information Disclosure	4499167	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Critical	Information Disclosure	4494441	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1023						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Critical	Information Disclosure	4494441	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Critical	Information Disclosure	4494441	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2019	4503327 Security Update	Moderate	Information Disclosure	4494441	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4503284 Security	Critical	Information Disclosure	4499179	Base: 6.5 Temporal: 5.9 Vector:	Yes

CVE-2019-1023						
10 Version 1709 for ARM64-based Systems	Update				CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Critical	Information Disclosure	4497936	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Critical	Information Disclosure	4497936	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	No
Microsoft Edge on Windows 10 Version	4503293 Security Update	Critical	Information Disclosure	4497936	Base: 6.5 Temporal: 5.9 Vector:	Yes

CVE-2019-1023						
1903 for ARM64-based Systems					CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
ChakraCore on ChakraCore	Release Notes Security Update	Critical	Information Disclosure	4497936	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-1024 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1024	**CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory	Critical	Remote Code Execution

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1024						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1024						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1024						
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1024						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1024						
Microsoft Edge on Windows Server 2019	4503327 Security Update	Moderate	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	No

CVE-2019-1024						
1903 for x64-based Systems						
Microsoft Edge on Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore on ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-1025 - Windows Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1025 MITRE NVD	**CVE Title:** Windows Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when Windows improperly handles objects in memory. An attacker who successfully exploited the vulnerability could cause a target system to stop responding. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application or to convince a user to open a specific file on a network share. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to cause a target system to stop responding. The update addresses the vulnerability by correcting how Windows handles objects in memory. **FAQ:** None **Mitigations:** None	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1025						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Denial of Service	4499164	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1025						
Windows 7 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Denial of Service	4499164	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/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 (Server Core installation)	4503269 Security Only 4503292 Monthly Rollup	Important	Denial of Service	4499164	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/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	4503269 Security Only 4503292 Monthly Rollup	Important	Denial of Service	4499164	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1025						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Denial of Service	4499164	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Denial of Service	4499149	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Important	Denial of Service	4499171	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1025						
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Important	Denial of Service	4499171	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4503290 Security Only 4503276 Monthly Rollup	Important	Denial of Service	4499151	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security Only	Important	Denial of Service	4499151	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security	Important	Denial of Service	4499151	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1025						
	Only					
Windows RT 8.1	4503276 Monthly Rollup	Important	Denial of Service	4499151	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Denial of Service	4499151	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4503291 Security Update	Important	Denial of Service	4499154	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Important	Denial of Service	4499154	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4503267 Security Update	Important	Denial of Service	4494440	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1025						
Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Important	Denial of Service	4494440	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Important	Denial of Service	4494440	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4503267 Security Update	Important	Denial of Service	4494440	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Denial of Service	4499181	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Denial of Service	4499181	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1025						
Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Important	Denial of Service	4499179	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Denial of Service	4499179	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Important	Denial of Service	4499167	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Denial of Service	4499167	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4503286 Security Update	Important	Denial of Service	4499167	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1025						
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Denial of Service	4499167	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Denial of Service	4494441	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Denial of Service	4494441	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Important	Denial of Service	4494441	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1025						
Windows Server 2019	4503327 Security Update	Important	Denial of Service	4494441	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4503327 Security Update	Important	Denial of Service	4494441	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Important	Denial of Service	4499179	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Important	Denial of Service	4497936	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Important	Denial of Service	4497936	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	No

CVE-2019-1025						
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Denial of Service	4497936	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Denial of Service	4497936	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	No
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Important	Denial of Service	4499149	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems	4503273 Monthly Rollup 4503287 Security	Important	Denial of Service	4499149	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1025						
Service Pack 2	Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Denial of Service	4499149	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Denial of Service	4499149	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1026 - Windows Audio Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1026 MITRE NVD	**CVE Title:** Windows Audio Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege exists in Windows Audio Service. An attacker who successfully exploited the vulnerability could run arbitrary code with elevated privileges. To exploit the vulnerability, an attacker could run a specially crafted application that could exploit the vulnerability. This vulnerability by itself does not allow arbitrary code to be run. However, this vulnerability could be used in conjunction with one or more vulnerabilities (e.g. a remote code execution vulnerability and another elevation of privilege) that could take advantage of the elevated privileges when running. The update addresses the vulnerability by correcting how the Windows Audio Service handles processes these requests. **FAQ:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1026						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1026						
Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1026						
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1026						
Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No

CVE-2019-1027 - Windows Audio Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1027 MITRE NVD	**CVE Title:** Windows Audio Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege exists in Windows Audio Service. An attacker who successfully exploited the vulnerability could run arbitrary code with elevated privileges. To exploit the vulnerability, an attacker could run a specially crafted application that could exploit the vulnerability. This vulnerability by itself does not allow arbitrary code to be run. However, this vulnerability could be used in conjunction with one or more vulnerabilities (e.g. a remote code execution vulnerability and another elevation of privilege) that could take advantage of the elevated privileges when running. The update addresses the vulnerability by correcting how the Windows Audio Service handles processes these requests. **FAQ:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1027						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1027						
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7	Yes

CVE-2019-1027						
ARM64-based Systems					Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1027						
Windows Server 2019 (Server Core installation)	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1027						
based Systems						
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No

CVE-2019-1028 - Windows Audio Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1028 MITRE NVD	**CVE Title:** Windows Audio Service Elevation of Privilege Vulnerability **Description:** An elevation of privilege exists in Windows Audio Service. An attacker who successfully exploited the vulnerability could run arbitrary code with elevated privileges.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, an attacker could run a specially crafted application that could exploit the vulnerability. This vulnerability by itself does not allow arbitrary code to be run. However, this vulnerability could be used in conjunction with one or more vulnerabilities (e.g. a remote code execution vulnerability and another elevation of privilege) that could take advantage of the elevated privileges when running. The update addresses the vulnerability by correcting how the Windows Audio Service handles processes these requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1028						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503269 Security Only 4503292	Important	Elevation of Privilege	4499164	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1028						
Systems Service Pack 1 (Server Core installation)	Monthly Rollup					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4503290 Security Only	Important	Elevation of Privilege	4499151	Base: 7.8 Temporal: 7	Yes

CVE-2019-1028						
	4503276 Monthly Rollup				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security Only	Important	Elevation of Privilege	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security Only	Important	Elevation of Privilege	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Important	Elevation of Privilege	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server	4503276 Monthly Rollup 4503290	Important	Elevation of Privilege	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1028						
Core installation)	Security Only					
Windows 10 for 32-bit Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1028						
Windows Server 2016 (Server Core installation)	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1028						
Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1028						
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1028						
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1028						
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No

CVE-2019-1029 - Skype for Business and Lync Server Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1029 MITRE NVD	**CVE Title:** Skype for Business and Lync Server Denial of Service Vulnerability **Description:** A denial of service vulnerability exists in Skype for Business. An attacker who successfully exploited the vulnerability could cause Skype for Business to stop responding. Note that the denial of service would not allow an attacker to execute code or to elevate the attacker's user rights.	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, an attacker needs to obtain a dial-in link for a vulnerable server and then initiates a series of calls within a short amount of time. The update addresses the vulnerability by correcting the way that Skype for Business server handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1029						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Lync Server 2010	4506009 Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Lync Server 2013	4506009 Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1031 - Microsoft Office SharePoint XSS Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1031 MITRE NVD	**CVE Title:** Microsoft Office SharePoint XSS Vulnerability **Description:** A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server.	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:** **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 06/11/2019 07:00:00		

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

Affected Software

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

CVE-2019-1031						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Foundation 2010 Service Pack 2	4464571 Security Update	Important	Spoofing	4464525	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Foundation 2013 Service Pack 1	4464597 Security Update	Important	Spoofing	4464511	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4464594 Security Update	Important	Spoofing	4464549	Base: N/A Temporal:	Maybe

CVE-2019-1031						
					N/A Vector: N/A	
Microsoft SharePoint Server 2019	4475512 Security Update	Important	Spoofing	4464556	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1032 - Microsoft Office SharePoint XSS Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1032 MITRE NVD	**CVE Title:** Microsoft Office SharePoint XSS Vulnerability **Description:** A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:** **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 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1032						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Enterprise Server 2016	4464594 Security Update	Important	Spoofing	4464549	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Server 2019	4475512 Security Update	Important	Spoofing	4464556	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1033 - Microsoft Office SharePoint XSS Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-	**CVE Title:** Microsoft Office SharePoint XSS Vulnerability **Description:**	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
1033 MITRE NVD	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:** **Is the Preview Pane an attack vector for this vulnerability?** No, the Preview Pane is not an attack vector. **Mitigations:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1033						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Project Server 2010 Service Pack 2	4092442 Security Update	Important	Spoofing	4022210	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1033						
Microsoft SharePoint Foundation 2013 Service Pack 1	4464602 Security Update	Important	Spoofing	4464564	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4464594 Security Update	Important	Spoofing	4464549	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Server 2019	4475512 Security Update	Important	Spoofing	4464556	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1034 - Microsoft Word Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1034	**CVE Title:** Microsoft Word Remote Code Execution Vulnerability **Description:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could use a specially crafted file to perform actions in the security context of the current user. For example, the file could then take actions on behalf of the logged-on user with the same permissions as the current user. To exploit the vulnerability, a user must open a specially crafted file with an affected version of Microsoft Word 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 that is designed to exploit the vulnerability. However, an attacker would have no way to force the user to visit the website. Instead, an attacker would have to convince the user to click a link, typically by way of an enticement in an email or Instant Messenger message, and then convince the user to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Word handles files in memory. **FAQ:** **Is the Preview Pane an attack vector for this vulnerability?**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	No, the Preview Pane is not an attack vector. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1034						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-1034						
Microsoft SharePoint Server 2010 Service Pack 2	4461611 Security Update	Important	Remote Code Execution	4461520	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (32-bit editions)	4461619 Security Update	Important	Remote Code Execution	4461526	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (64-bit editions)	4461619 Security Update	Important	Remote Code Execution	4461526	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4462178 Security Update	Important	Remote Code Execution	4461617	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4462178 Security Update	Important	Remote Code Execution	4461617	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Web Apps 2010 Service Pack 2	4461621 Security Update	Important	Remote Code Execution	4461527	Base: N/A Temporal:	Maybe

CVE-2019-1034						
					N/A Vector: N/A	
Microsoft Word 2013 Service Pack 1 (32-bit editions)	4464590 Security Update	Important	Remote Code Execution	4461594	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (64-bit editions)	4464590 Security Update	Important	Remote Code Execution	4461594	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 RT Service Pack 1	4464590 Security Update	Important	Remote Code Execution	4461594	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 for Mac	Release Notes Security Update	Important	Remote Code Execution	4461594	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Word 2016 (32-bit edition)	4464596 Security Update	Important	Remote Code Execution	4464536	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1034						
Microsoft Word 2016 (64-bit edition)	4464596 Security Update	Important	Remote Code Execution	4464536	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4464594 Security Update	Important	Remote Code Execution	4464549	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2013 Service Pack 1	4464602 Security Update	Important	Remote Code Execution	4464564	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2019 for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution	4464564	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office 2019 for 64-bit editions	Click to Run Security Update	Important	Remote Code Execution	4464564	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office 2019 for Mac	Release Notes Security Update	Important	Remote Code Execution	4464564	Base: N/A Temporal:	No

CVE-2019-1034						
					N/A Vector: N/A	
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Remote Code Execution	4464564	Base: N/A Temporal: N/A Vector: N/A	No
Office 365 ProPlus for 64-bit Systems	Click to Run Security Update	Important	Remote Code Execution	4464564	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft SharePoint Server 2019	4475512 Security Update	Important	Remote Code Execution	4464556	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Online Server	4475511 Security Update	Important	Remote Code Execution	4462169	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1035 - Microsoft Word Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1035 MITRE NVD	**CVE Title:** Microsoft Word Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could use a specially crafted file to perform actions in the security context of the current user. For example, the file could then take actions on behalf of the logged-on user with the same permissions as the current user. To exploit the vulnerability, a user must open a specially crafted file with an affected version of Microsoft Word 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 that is designed to exploit the vulnerability. However, an attacker would have no way to force the user to visit the website. Instead, an attacker would have to convince the user to click a link, typically by way of an enticement in an email or Instant Messenger message, and then convince the user to open the specially crafted file.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how Microsoft Word handles files 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 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1035						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2016 for Mac	Release Notes Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office 2019 for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office 2019 for 64-bit editions	Click to Run Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office 2019 for Mac	Release Notes Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	No

CVE-2019-1035						
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	No
Office 365 ProPlus for 64-bit Systems	Click to Run Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	No
Microsoft SharePoint Server 2019	4475512 Security Update	Important	Remote Code Execution	4464556	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Online Server	4475511 Security Update	Important	Remote Code Execution	4462169	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1036 - Microsoft Office SharePoint XSS Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1036 MITRE NVD	**CVE Title:** Microsoft Office SharePoint XSS Vulnerability **Description:** A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:**	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1036						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-1036						
Microsoft Project Server 2010 Service Pack 2	4092442 Security Update	Important	Spoofing	4022210	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Foundation 2013 Service Pack 1	4464602 Security Update	Important	Spoofing	4464564	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4464594 Security Update	Important	Spoofing	4464549	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Server 2019	4475512 Security Update	Important	Spoofing	4464556	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1038 - Microsoft Browser Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1038 MITRE NVD	**CVE Title:** Microsoft Browser Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory. The vulnerability could corrupt memory in a way that could allow an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, the attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. An attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft browsers, and then convince a user to view the website. The attacker could also take advantage of compromised websites, or websites that accept or host user-provided content or advertisements, by adding specially crafted content that could exploit the vulnerability. In all cases, however, 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 via an enticement in email or instant message, or by getting them to open an email attachment.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by modifying how Microsoft browsers handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1038						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4503292 Monthly Rollup 4503259 IE Cumulative	Critical	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7 Vector: CVSS: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 7 for x64-based Systems Service Pack 1	4503292 Monthly Rollup 4503259 IE Cumulative	Critical	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1038						
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503292 Monthly Rollup 4503259 IE Cumulative	Moderate	Remote Code Execution	4498206	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	4503259 IE Cumulative	Moderate	Remote Code Execution	4498206	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 8.1 for	4503276 Monthly Rollup 4503259 IE Cumulative	Critical	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1038						
32-bit systems						
Internet Explorer 11 on Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503259 IE Cumulative	Critical	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4503276 Monthly Rollup	Moderate	Remote Code Execution	4499151	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 RT 8.1	4503276 Monthly Rollup	Critical	Remote Code Execution	4499151	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1038						
Internet Explorer 11 on Windows 10 for 32-bit Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2016	4503267 Security Update	Moderate	Remote Code Execution	4494440	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-2019-1038						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 7.5 Temporal: 6.7 Vector: CVSS: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 x64-based Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1038						
10 Version 1703 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1038						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1038						
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-1038						
Windows 10 Version 1809 for 32-bit Systems					Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1038						
ARM64-based Systems						
Internet Explorer 11 on Windows Server 2019	4503327 Security Update	Moderate	Remote Code Execution	4494441	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 ARM64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1038						
10 Version 1903 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1038						
based Systems						
Internet Explorer 10 on Windows Server 2012	4503285 Monthly Rollup 4503259 IE Cumulative	Moderate	Remote Code Execution	4498206	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
Microsoft Edge on Windows 10 for 32-bit Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1038						
Microsoft Edge on Windows Server 2016	4503267 Security Update	Moderate	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1038						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1038						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1038						
Version 1803 for x64-based Systems						
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1038						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2019	4503327 Security Update	Moderate	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1038						
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1903 for	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	No

CVE-2019-1038						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1039 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1039	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory. To exploit this vulnerability, an authenticated attacker could run a specially crafted application. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system. The update addresses the vulnerability by correcting how the Windows kernel initializes 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		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1039						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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-	4503269 Security	Important	Information Disclosure	4499164	Base: 5.5 Temporal: 5	Yes

CVE-2019-1039						
based Systems Service Pack 1	Only 4503292 Monthly 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 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1039						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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)	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4503263 Security Only 4503285 Monthly Rollup	Important	Information Disclosure	4499171	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1039						
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Important	Information Disclosure	4499171	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4503290 Security Only 4503276 Monthly Rollup	Important	Information Disclosure	4499151	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4503276 Monthly Rollup 4503290 Security Only	Important	Information Disclosure	4499151	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4503276 Monthly Rollup 4503290 Security	Important	Information Disclosure	4499151	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1039						
	Only					
Windows RT 8.1	4503276 Monthly Rollup	Important	Information Disclosure	4499151	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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)	4503276 Monthly Rollup 4503290 Security Only	Important	Information Disclosure	4499151	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4503291 Security Update	Important	Information Disclosure	4499154	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4503291 Security Update	Important	Information Disclosure	4499154	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1039						
Windows Server 2016	4503267 Security Update	Important	Information Disclosure	4494440	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4503267 Security Update	Important	Information Disclosure	4494440	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4503267 Security Update	Important	Information Disclosure	4494440	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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)	4503267 Security Update	Important	Information Disclosure	4494440	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4503279 Security	Important	Information Disclosure	4499181	Base: 5.5 Temporal: 5	Yes

CVE-2019-1039						
1703 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 1703 for x64-based Systems	4503279 Security Update	Important	Information Disclosure	4499181	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4503284 Security Update	Important	Information Disclosure	4499179	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4503284 Security Update	Important	Information Disclosure	4499179	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4503286 Security Update	Important	Information Disclosure	4499167	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1039						
Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Information Disclosure	4499167	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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)	4503286 Security Update	Important	Information Disclosure	4499167	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4503286 Security Update	Important	Information Disclosure	4499167	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4503327 Security Update	Important	Information Disclosure	4494441	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2019-1039						
32-bit Systems					CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Information Disclosure	4494441	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4503327 Security Update	Important	Information Disclosure	4494441	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4503327 Security Update	Important	Information Disclosure	4494441	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4503327 Security Update	Important	Information Disclosure	4494441	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1039						
Core installation)						
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Important	Information Disclosure	4499179	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4503293 Security Update	Important	Information Disclosure	4497936	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4503293 Security Update	Important	Information Disclosure	4497936	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-	4503293 Security Update	Important	Information Disclosure	4497936	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1039						
based Systems						
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Information Disclosure	4497936	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	No
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Important	Information Disclosure	4499149	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1039						
Service Pack 2						
Windows Server 2008 for x64-based Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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)	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1040 - Windows NTLM Tampering Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1040 MITRE NVD	**CVE Title:** Windows NTLM Tampering Vulnerability **Description:** A tampering vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLM MIC (Message Integrity Check) protection. An attacker who successfully exploited this vulnerability could gain the ability to downgrade NTLM security features. To exploit this vulnerability, the attacker would need to tamper with the NTLM exchange. The attacker could then modify flags of the NTLM packet without invalidating the signature. The update addresses the vulnerability by hardening NTLM MIC protection on the server-side. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Tampering

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1040						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292	Important	Tampering	4499164	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1040						
	Monthly Rollup					
Windows 7 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Tampering	4499164	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4503269 Security Only 4503292 Monthly Rollup	Important	Tampering	4499164	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for	4503269 Security	Important	Tampering	4499164	Base: 5.3 Temporal: 4.8 Vector:	Yes

CVE-2019-1040						
Itanium-Based Systems Service Pack 1	Only 4503292 Monthly Rollup				CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Tampering	4499164	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Tampering	4499149	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1040						
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Important	Tampering	4499171	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Important	Tampering	4499171	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4503290 Security Only 4503276 Monthly	Important	Tampering	4499151	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1040						
	Rollup					
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security Only	Important	Tampering	4499151	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security Only	Important	Tampering	4499151	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Important	Tampering	4499151	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1040						
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Tampering	4499151	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4503291 Security Update	Important	Tampering	4499154	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Important	Tampering	4499154	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4503267 Security Update	Important	Tampering	4494440	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1040						
Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Important	Tampering	4494440	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Important	Tampering	4494440	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4503267 Security Update	Important	Tampering	4494440	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Tampering	4499181	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version	4503279	Important	Tampering	4499181	Base: 5.3 Temporal: 4.8	Yes

CVE-2019-1040						
1703 for x64-based Systems	Security Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Important	Tampering	4499179	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Tampering	4499179	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Important	Tampering	4499167	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Tampering	4499167	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1040						
Windows Server, version 1803 (Server Core Installation)	4503286 Security Update	Important	Tampering	4499167	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Tampering	4499167	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Tampering	4494441	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for	4503327 Security Update	Important	Tampering	4494441	Base: 5.3 Temporal: 4.8 Vector:	Yes

CVE-2019-1040						
x64-based Systems					CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Important	Tampering	4494441	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4503327 Security Update	Important	Tampering	4494441	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4503327 Security Update	Important	Tampering	4494441	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-	4503284 Security Update	Important	Tampering	4499179	Base: 5.3 Temporal: 4.8 Vector:	Yes

CVE-2019-1040						
based Systems					CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Important	Tampering	4497936	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Important	Tampering	4497936	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Tampering	4497936	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server	4503293 Security Update	Important	Tampering	4497936	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	No

CVE-2019-1040						
Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Important	Tampering	4499149	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Tampering	4499149	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4503273 Monthly Rollup 450328	Important	Tampering	4499149	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1040						
Service Pack 2	7 Security Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Tampering	4499149	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1041 - Windows Kernel Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-	**CVE Title:** Windows Kernel Elevation of Privilege Vulnerability **Description:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
1041 MITRE NVD	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application to take control of an affected system. The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1041						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1041						
Core Installation)						
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1041						
based Systems						
Windows Server 2019	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No

CVE-2019-1041						
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No

CVE-2019-1043 - Comctl32 Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-	**CVE Title:** Comctl32 Remote Code Execution Vulnerability **Description:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
1043 MITRE NVD	A remote code execution vulnerability exists in the way that comctl32.dll 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, the attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. An attacker could host a specially crafted website designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. The attacker could also take advantage of compromised websites, or websites that accept or host user-provided content or advertisements, by adding specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action, typically by an enticement in an email or instant message, or by getting the user to open an attachment sent through email. The security update addresses the vulnerability by modifying how comctl32.dll handles objects in memory. **FAQ:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1043						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems	4503269 Security Only 4503292	Important	Remote Code Execution	4499164	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-2019-1043						
Service Pack 1	Monthly Rollup					
Windows 7 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based	4503269 Security Only 4503292 Monthly	Important	Remote Code Execution	4499164	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-2019-1043						
Systems Service Pack 1	Rollup					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Remote Code Execution	4499164	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4503263 Security Only	Important	Remote Code Execution	4499171	Base: 6.4 Temporal: 5.8	Yes

CVE-2019-1043						
	4503285 Monthly Rollup				Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Important	Remote Code Execution	4499171	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4503290 Security Only 4503276 Monthly Rollup	Important	Remote Code Execution	4499151	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security Only	Important	Remote Code Execution	4499151	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-2019-1043						
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security Only	Important	Remote Code Execution	4499151	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Important	Remote Code Execution	4499151	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Remote Code Execution	4499151	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4503291 Security Update	Important	Remote Code Execution	4499154	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-	4503291 Security Update	Important	Remote Code Execution	4499154	Base: 6.4 Temporal: 5.8	Yes

CVE-2019-1043						
based Systems					Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2016	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Important	Remote Code Execution	4494440	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4503267 Security Update	Important	Remote Code Execution	4494440	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-2019-1043						
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Remote Code Execution	4499181	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Remote Code Execution	4499181	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 6.4 Temporal: 5.8	Yes

CVE-2019-1043						
32-bit Systems					Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Remote Code Execution	4499167	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 6.4 Temporal: 5.8	Yes

CVE-2019-1043						
32-bit Systems					Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4503327 Security Update	Important	Remote Code Execution	4494441	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4503327 Security Update	Important	Remote Code Execution	4494441	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-2019-1043						
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Important	Remote Code Execution	4499179	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Important	Remote Code Execution	4497936	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Important	Remote Code Execution	4497936	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	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Remote Code Execution	4497936	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-2019-1043						
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Remote Code Execution	4497936	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	No
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Important	Remote Code Execution	4499149	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	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-2019-1043						
Windows Server 2008 for x64-based Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Remote Code Execution	4499149	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-2019-1044 - Windows Secure Kernel Mode Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1044 MITRE NVD	**CVE Title:** Windows Secure Kernel Mode Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists when Windows Secure Kernel Mode fails to properly handle objects in memory. To exploit the vulnerability, a locally-authenticated attacker could attempt to run a specially crafted application on a targeted system. An attacker who successfully exploited the vulnerability could violate virtual trust levels (VTL). The update addresses the vulnerability by correcting how Windows Secure Kernel Mode handles objects in memory to properly enforce VTLs. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1044						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Security Feature Bypass	4494441	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-	4503327 Security Update	Important	Security Feature Bypass	4494441	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1044						
based Systems						
Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Important	Security Feature Bypass	4494441	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2019	4503327 Security Update	Important	Security Feature Bypass	4494441	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4503327 Security Update	Important	Security Feature Bypass	4494441	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1045 - Windows Network File System Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1045 MITRE NVD	**CVE Title:** Windows Network File System Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way that the Windows Network File System (NFS) handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application. The security update addresses the vulnerability by ensuring the Windows NFS properly handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1045						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1045						
Windows 7 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1045						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Important	Elevation of Privilege	4499171	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Important	Elevation of Privilege	4499171	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4503290 Security Only 4503276	Important	Elevation of Privilege	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1045						
	Monthly Rollup					
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security Only	Important	Elevation of Privilege	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security Only	Important	Elevation of Privilege	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Important	Elevation of Privilege	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security	Important	Elevation of Privilege	4499151	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1045						
	Only					
Windows 10 for 32-bit Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1045						
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1046 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1046	**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	Important	Information Disclosure

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1046						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1046						
	Rollup					
Windows 7 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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)	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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-	4503269 Security Only	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-1046						
Based Systems Service Pack 1	4503292 Monthly Rollup				CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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)	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1046						
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Important	Information Disclosure	4499171	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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)	4503263 Security Only 4503285 Monthly Rollup	Important	Information Disclosure	4499171	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503290 Security Only 4503276 Monthly	Important	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1046						
	Rollup					
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security Only	Important	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security Only	Important	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Important	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1046						
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503291 Security Update	Important	Information Disclosure	4499154	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503291 Security Update	Important	Information Disclosure	4499154	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4503267 Security Update	Important	Information Disclosure	4494440	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1046						
Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Important	Information Disclosure	4494440	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503267 Security Update	Important	Information Disclosure	4494440	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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)	4503267 Security Update	Important	Information Disclosure	4494440	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Information Disclosure	4499181	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1046						
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Information Disclosure	4499181	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503284 Security Update	Important	Information Disclosure	4499179	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503284 Security Update	Important	Information Disclosure	4499179	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503286 Security Update	Important	Information Disclosure	4499167	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for	4503286 Security	Important	Information Disclosure	4499167	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-1046						
x64-based Systems	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4503286 Security Update	Important	Information Disclosure	4499167	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503286 Security Update	Important	Information Disclosure	4499167	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1046						
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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)	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1046						
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Important	Information Disclosure	4499179	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503293 Security Update	Important	Information Disclosure	4497936	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503293 Security Update	Important	Information Disclosure	4497936	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Information Disclosure	4497936	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1046						
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Information Disclosure	4497936	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	No
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1046						
Windows Server 2008 for x64-based Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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)	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1047 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1047 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.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1047						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-1047						
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1047						
(Server Core installation)	Rollup					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for	4503273 Monthly	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-1047						
32-bit Systems Service Pack 2 (Server Core installation)	Rollup 4503287 Security Only				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503273 Monthly Rollup 4503287 Security	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1047						
	Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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)	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1048 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1048 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.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1048						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-1048						
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1048						
(Server Core installation)	Rollup					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for	4503273 Monthly	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-1048						
32-bit Systems Service Pack 2 (Server Core installation)	Rollup 4503287 Security Only				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503273 Monthly Rollup 4503287 Security	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1048						
	Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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)	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1049 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1049 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.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1049						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-1049						
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1049						
(Server Core installation)	Rollup					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503269 Security Only 4503292 Monthly Rollup	Important	Information Disclosure	4499164	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for	4503273 Monthly	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-1049						
32-bit Systems Service Pack 2 (Server Core installation)	Rollup 4503287 Security Only				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4503287 Security Only 4503273 Monthly Rollup	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503273 Monthly Rollup 4503287 Security	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1049						
	Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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)	4503273 Monthly Rollup 4503287 Security Only	Important	Information Disclosure	4499149	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1050 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1050 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.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1050						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-1050						
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Important	Information Disclosure	4499171	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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)	4503263 Security Only 4503285 Monthly Rollup	Important	Information Disclosure	4499171	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503290 Security Only 4503276 Monthly	Important	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1050						
	Rollup					
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security Only	Important	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security Only	Important	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Important	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1050						
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Information Disclosure	4499151	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503291 Security Update	Important	Information Disclosure	4499154	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503291 Security Update	Important	Information Disclosure	4499154	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4503267 Security Update	Important	Information Disclosure	4494440	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1050						
Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Important	Information Disclosure	4494440	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503267 Security Update	Important	Information Disclosure	4494440	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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)	4503267 Security Update	Important	Information Disclosure	4494440	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Information Disclosure	4499181	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1050						
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Information Disclosure	4499181	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503284 Security Update	Important	Information Disclosure	4499179	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503284 Security Update	Important	Information Disclosure	4499179	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503286 Security Update	Important	Information Disclosure	4499167	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for	4503286 Security	Important	Information Disclosure	4499167	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-1050						
x64-based Systems	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4503286 Security Update	Important	Information Disclosure	4499167	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503286 Security Update	Important	Information Disclosure	4499167	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1050						
Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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)	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1050						
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Important	Information Disclosure	4499179	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503293 Security Update	Important	Information Disclosure	4497936	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/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	4503293 Security Update	Important	Information Disclosure	4497936	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Information Disclosure	4497936	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1050						
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Information Disclosure	4497936	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	No

CVE-2019-1051 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1051 MITRE NVD	**CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00		

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

Affected Software

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

CVE-2019-1051						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1051						
based Systems						
Microsoft Edge on Windows Server 2016	4503267 Security Update	Moderate	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-1051						
10 Version 1703 for 32-bit Systems					Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1051						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for ARM64-	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1051						
based Systems						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1051						
based Systems						
Microsoft Edge on Windows Server 2019	4503327 Security Update	Moderate	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1051						
Microsoft Edge on Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	No
Microsoft Edge on Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore on ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-1052 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1052 MITRE NVD	**CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1052						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2016	4503267 Security Update	Moderate	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1052						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1052						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1052						
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1052						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2019	4503327 Security Update	Moderate	Remote Code Execution	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1052						
1709 for ARM64-based Systems						
Microsoft Edge on Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	No
Microsoft Edge on Windows 10 Version 1903 for	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1052						
ARM64-based Systems						
ChakraCore on ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-1053 - Windows Shell Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1053 MITRE NVD	**CVE Title:** Windows Shell Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows Shell fails to validate folder shortcuts. An attacker who successfully exploited the vulnerability could elevate privileges by escaping a sandbox. To exploit this vulnerability, an attacker would require unprivileged execution on the victim system.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correctly validating folder shortcuts. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1053						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-1053						
Windows 7 for 32-bit Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1053						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503269 Security Only 4503292 Monthly Rollup	Important	Elevation of Privilege	4499164	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1053						
Windows Server 2012	4503263 Security Only 4503285 Monthly Rollup	Important	Elevation of Privilege	4499171	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4503263 Security Only 4503285 Monthly Rollup	Important	Elevation of Privilege	4499171	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4503290 Security Only 4503276 Monthly Rollup	Important	Elevation of Privilege	4499151	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503290 Security	Important	Elevation of Privilege	4499151	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1053						
	Only					
Windows Server 2012 R2	4503276 Monthly Rollup 4503290 Security Only	Important	Elevation of Privilege	4499151	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4503276 Monthly Rollup	Important	Elevation of Privilege	4499151	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4503276 Monthly Rollup 4503290 Security Only	Important	Elevation of Privilege	4499151	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1053						
Windows 10 for x64-based Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2016	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1053						
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1053						
Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1053						
based Systems						
Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2019	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 6.3 Temporal: 5.7	Yes

CVE-2019-1053						
for 32-bit Systems					Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	
Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	No
Windows Server 2008 for Itanium-Based Systems	4503287 Security Only 4503273 Monthly Rollup	Important	Elevation of Privilege	4499149	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1053						
Service Pack 2						
Windows Server 2008 for 32-bit Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server	4503273 Monthly Rollup 4503287 Security Only	Important	Elevation of Privilege	4499149	Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1053						
Core installation)						

CVE-2019-1054 - Microsoft Edge Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1054 MITRE NVD	**CVE Title:** Microsoft Edge Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists in Edge that allows for bypassing Mark of the Web Tagging (MOTW). Failing to set the MOTW means that a large number of Microsoft security technologies are bypassed. In a web-based attack scenario, an attacker could host a malicious website that is designed to exploit the security feature bypass. Alternatively, in an email or instant message attack scenario, the attacker could send the targeted user a specially crafted .url file that is designed to exploit the bypass. Additionally, compromised websites or websites that accept or host user-provided content could contain specially crafted content to exploit the security feature bypass. However, in all cases an attacker would have no way to force a user to view attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	entice a user to either click a link that directs the user to the attacker's site or send a malicious attachment. The security update addresses the security feature bypass by correcting how Edge handles MOTW tagging. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1054						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows Server 2016	4503267 Security Update	Low	Security Feature Bypass	4494440	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Important	Security Feature Bypass	4494440	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Important	Security Feature Bypass	4494440	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4503279 Security Update	Important	Security Feature Bypass	4499181	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1054						
1703 for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Security Feature Bypass	4499181	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Important	Security Feature Bypass	4499179	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Security Feature Bypass	4499179	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1054						
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Important	Security Feature Bypass	4499167	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Security Feature Bypass	4499167	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Security Feature Bypass	4499167	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1054						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Security Feature Bypass	4494441	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Security Feature Bypass	4494441	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Important	Security Feature Bypass	4494441	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1054						
Microsoft Edge on Windows Server 2019	4503327 Security Update	Low	Security Feature Bypass	4494441	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Important	Security Feature Bypass	4499179	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Important	Security Feature Bypass	4497936	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1903 for	4503293 Security Update	Important	Security Feature Bypass	4497936	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	No

CVE-2019-1054						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Security Feature Bypass	4497936	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-1055 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1055 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 designed to exploit the vulnerability through a Microsoft browser and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the browser rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1055						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows Server 2008 for 32-bit	4503273 Monthly Rollup 4503259 IE Cumulative	Moderate	Remote Code Execution	4498206	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-2019-1055						
Systems Service Pack 2						
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4503287 Security Only 4503259 IE Cumulative	Moderate	Remote Code Execution	4498206	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	4503292 Monthly Rollup 4503259 IE Cumulative	Critical	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1055						
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4503292 Monthly Rollup 4503259 IE Cumulative	Critical	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503292 Monthly Rollup 4503259 IE Cumulative	Moderate	Remote Code Execution	4498206	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-2019-1055						
Internet Explorer 11 on Windows Server 2012	4503259 IE Cumulative	Moderate	Remote Code Execution	4498206	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 8.1 for 32-bit systems	4503276 Monthly Rollup 4503259 IE Cumulative	Critical	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503276 Monthly Rollup 4503259 IE Cumulative	Critical	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1055						
Internet Explorer 11 on Windows Server 2012 R2	4503276 Monthly Rollup 4503259 IE Cumulative	Moderate	Remote Code Execution	4498206	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 RT 8.1	4503276 Monthly Rollup	Critical	Remote Code Execution	4499151	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1055						
x64-based Systems						
Internet Explorer 11 on Windows Server 2016	4503267 Security Update	Moderate	Remote Code Execution	4494440	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 1607 for 32-bit Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1055						
Version 1607 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 7.5 Temporal: 6.7 Vector: CVSS: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 1703 for x64-	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1055						
based Systems						
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1055						
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1055						
10 Version 1803 for ARM64-based Systems						
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 7.5 Temporal: 6.7 Vector: CVSS: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 x64-	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1055						
based Systems						
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2019	4503327 Security Update	Moderate	Remote Code Execution	4494441	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	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1055						
Version 1709 for ARM64-based Systems						
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1903 for x64-	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No

CVE-2019-1055						
based Systems						
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 7.5 Temporal: 6.7 Vector: CVSS: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 10 on Windows Server 2012	4503285 Monthly Rollup 4503259 IE Cumulative	Moderate	Remote Code Execution	4498206	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-2019-1064 - Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1064 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 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1064						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2016	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7	Yes

CVE-2019-1064						
1607 for 32-bit Systems					Vector: CVSS: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 1607 for x64-based Systems	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7	Yes

CVE-2019-1064						
1709 for 32-bit Systems					Vector: CVSS: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 1709 for x64-based Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1064						
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1064						
Windows Server 2019	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No

CVE-2019-1064						
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No

CVE-2019-1065 - Windows Kernel Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1065	**CVE Title:** Windows Kernel Elevation of Privilege Vulnerability **Description:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application to take control of an affected system. The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1065						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1065						
Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1065						
Windows Server 2019	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1065						
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No

CVE-2019-1069 - Task Scheduler Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1069 MITRE NVD	**CVE Title:** Task Scheduler Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way the Task Scheduler Service validates certain file operations. An attacker who successfully exploited the vulnerability could gain elevated privileges on a victim system. To exploit the vulnerability, an attacker would require unprivileged code execution on a victim system. The security update addresses the vulnerability by correctly validating file operations.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1069						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-1069						
Windows 10 for 32-bit Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4503291 Security Update	Important	Elevation of Privilege	4499154	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1069						
Windows Server 2016 (Server Core installation)	4503267 Security Update	Important	Elevation of Privilege	4494440	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Elevation of Privilege	4499181	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1069						
Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503286 Security Update	Important	Elevation of Privilege	4499167	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1069						
Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4503327 Security Update	Important	Elevation of Privilege	4494441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1069						
Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Important	Elevation of Privilege	4499179	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/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	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1069						
Windows Server, version 1903 (Server Core installation)	4503293 Security Update	Important	Elevation of Privilege	4497936	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No

CVE-2019-1080 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1080 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers. 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	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 designed to exploit the vulnerability through a Microsoft browser and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the browser 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 06/11/2019 07:00:00		

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

Affected Software

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

CVE-2019-1080						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	4503273 Monthly Rollup 4503259 IE Cumulative	Moderate	Remote Code Execution	4498206	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-2019-1080						
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4503273 Monthly Rollup 4503259 IE Cumulative	Moderate	Remote Code Execution	4498206	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	4503292 Monthly Rollup 4503259 IE Cumulative	Critical	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503292 Monthly Rollup	Critical	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-1080						
Windows 7 for x64-based Systems Service Pack 1	4503259 IE Cumulative				Vector: CVSS: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	4503292 Monthly Rollup 4503259 IE Cumulative	Moderate	Remote Code Execution	4498206	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	4503259 IE Cumulative	Moderate	Remote Code Execution	4498206	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-2019-1080						
Server 2012						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4503276 Monthly Rollup 4503259 IE Cumulative	Critical	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503290 Security Only 4503259 IE Cumulative	Critical	Remote Code Execution	4498206	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4503290 Security Only 4503259 IE Cumulative	Moderate	Remote Code Execution	4498206	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-2019-1080						
Internet Explorer 11 on Windows RT 8.1	4503276 Monthly Rollup	Critical	Remote Code Execution	4499151	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4503291 Security Update	Critical	Remote Code Execution	4499154	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503267 Security Update	Moderate	Remote Code Execution	4494440	Base: 6.4 Temporal: 5.8	Yes

CVE-2019-1080						
Windows Server 2016					Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 7.5 Temporal: 6.7 Vector: CVSS: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 x64-based Systems	4503267 Security Update	Critical	Remote Code Execution	4494440	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1080						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 7.5 Temporal: 6.7 Vector: CVSS: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 1703 for x64-based Systems	4503279 Security Update	Critical	Remote Code Execution	4499181	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1080						
10 Version 1709 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1080						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Critical	Remote Code Execution	4499167	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1080						
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 7.5 Temporal: 6.7 Vector: CVSS: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 x64-based Systems	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 7.5 Temporal: 6.7 Vector: CVSS: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	4503327 Security Update	Critical	Remote Code Execution	4494441	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1080						
10 Version 1809 for ARM64-based Systems						
Internet Explorer 11 on Windows Server 2019	4503327 Security Update	Moderate	Remote Code Execution	4494441	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 ARM64-based Systems	4503284 Security Update	Critical	Remote Code Execution	4499179	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1080						
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	No
Internet Explorer 11 on Windows	4503293 Security Update	Critical	Remote Code Execution	4497936	Base: 7.5 Temporal: 6.7 Vector: CVSS: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-2019-1080						
10 Version 1903 for ARM64-based Systems						
Internet Explorer 10 on Windows Server 2012	4503285 Monthly Rollup 4503259 IE Cumulative	Moderate	Remote Code Execution	4498206	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-2019-1081 - Microsoft Browser Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1081 MITRE NVD	**CVE Title:** Microsoft Browser Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when affected Microsoft browsers improperly 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, in a web-based attack scenario, an attacker could host a website that is used to attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site. The security update addresses the vulnerability by modifying how Microsoft browsers handle objects in memory.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 06/11/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1081						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	4503273 Monthly Rollup 4503259 IE Cumulative	Low	Information Disclosure	4498206	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes
Internet Explorer 9 on Windows Server 2008 for x64-based Systems	4503273 Monthly Rollup 4503259 IE Cumulative	Low	Information Disclosure	4498206	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes

CVE-2019-1081						
Service Pack 2						
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4503292 Monthly Rollup 4503259 IE Cumulative	Important	Information Disclosure	4498206	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4503292 Monthly Rollup 4503259 IE Cumulative	Important	Information Disclosure	4498206	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes

CVE-2019-1081						
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4503292 Monthly Rollup 4503259 IE Cumulative	Low	Information Disclosure	4498206	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows Server 2012	4503259 IE Cumulative	Low	Information Disclosure	4498206	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows 8.1 for	4503276 Monthly Rollup 4503259 IE Cumulative	Important	Information Disclosure	4498206	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes

CVE-2019-1081						
32-bit systems						
Internet Explorer 11 on Windows 8.1 for x64-based systems	4503276 Monthly Rollup 4503259 IE Cumulative	Important	Information Disclosure	4498206	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows Server 2012 R2	4503276 Monthly Rollup 4503259 IE Cumulative	Low	Information Disclosure	4498206	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows RT 8.1	4503276 Monthly Rollup	Important	Information Disclosure	4499151	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes

CVE-2019-1081						
Internet Explorer 11 on Windows 10 for 32-bit Systems	4503291 Security Update	Important	Information Disclosure	4499154	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4503291 Security Update	Important	Information Disclosure	4499154	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows Server 2016	4503267 Security Update	Low	Information Disclosure	4494440	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes

CVE-2019-1081						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Important	Information Disclosure	4494440	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4503267 Security Update	Important	Information Disclosure	4494440	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows	4503279 Security Update	Important	Information Disclosure	4499181	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes

CVE-2019-1081						
10 Version 1703 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Information Disclosure	4499181	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 Version 1709 for	4503284 Security Update	Important	Information Disclosure	4499179	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes

CVE-2019-1081						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Information Disclosure	4499179	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4503286 Security Update	Important	Information Disclosure	4499167	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes

CVE-2019-1081						
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Information Disclosure	4499167	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems	4503286 Security Update	Important	Information Disclosure	4499167	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes
Internet Explorer 11 on	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.3 Temporal: 3.9	Yes

CVE-2019-1081						
Windows 10 Version 1809 for 32-bit Systems					Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 Version 1809 for	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes

CVE-2019-1081						
ARM64-based Systems						
Internet Explorer 11 on Windows Server 2019	4503327 Security Update	Low	Information Disclosure	4494441	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems	4503284 Security Update	Important	Information Disclosure	4499179	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows	4503293 Security Update	Important	Information Disclosure	4497936	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes

CVE-2019-1081						
10 Version 1903 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Important	Information Disclosure	4497936	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	No
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-	4503293 Security Update	Important	Information Disclosure	4497936	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes

CVE-2019-1081						
based Systems						
Internet Explorer 10 on Windows Server 2012	4503285 Monthly Rollup 4503259 IE Cumulative	Low	Information Disclosure	4498206	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes
Microsoft Edge on Windows 10 for 32-bit Systems	4503291 Security Update	Important	Information Disclosure	4499154	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4503291 Security Update	Important	Information Disclosure	4499154	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1081						
Microsoft Edge on Windows Server 2016	4503267 Security Update	Low	Information Disclosure	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4503267 Security Update	Important	Information Disclosure	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-	4503267 Security Update	Important	Information Disclosure	4494440	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1081						
based Systems						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4503279 Security Update	Important	Information Disclosure	4499181	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4503279 Security Update	Important	Information Disclosure	4499181	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1081						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4503284 Security Update	Important	Information Disclosure	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4503284 Security Update	Important	Information Disclosure	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4503286 Security Update	Important	Information Disclosure	4499167	Base: 4.2 Temporal: 3.8 Vector:	Yes

CVE-2019-1081						
10 Version 1803 for 32-bit Systems					CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4503286 Security Update	Important	Information Disclosure	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for ARM64-	4503286 Security Update	Important	Information Disclosure	4499167	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1081						
based Systems						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1081						
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4503327 Security Update	Important	Information Disclosure	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2019	4503327 Security Update	Low	Information Disclosure	4494441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for	4503284 Security Update	Important	Information Disclosure	4499179	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-1081						
ARM64-based Systems						
Microsoft Edge on Windows 10 Version 1903 for 32-bit Systems	4503293 Security Update	Important	Information Disclosure	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1903 for x64-based Systems	4503293 Security Update	Important	Information Disclosure	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	No

CVE-2019-1081						
Microsoft Edge on Windows 10 Version 1903 for ARM64-based Systems	4503293 Security Update	Important	Information Disclosure	4497936	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

声 明

==========

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。

关于绿盟科技

==========

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）成立于 2000 年 4 月，总部位于北京。在国内外设有 30 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测/防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易，股票简称：绿盟科技，股票代码：300369。

绿盟科技官方微博二维码

绿盟科技官方微信二维码