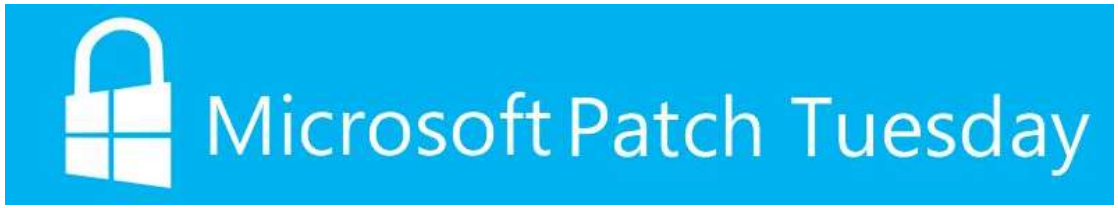
Microsoft Security Bulletin for February 2019 Patches That Fix 79 Security Vulnerabilities



Date of Release: Feburary 13, 2019

Overview

Microsoft released the January 2019 security patch on Tuesday that fixes 79 vulnerabilities ranging from simple spoofing attacks to remote code execution in various products, including .NET Framework, Adobe Flash Player, Azure, Internet Explorer, Microsoft Browsers, 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, Team Foundation Server, Visual Studio, Windows DHCP Server, Windows Hyper-V, Windows Kernel, and Windows SMB Server.

Details can be found in the following table.

Product	CVE ID	CVE Title	Severity Level
.NET Framework	CVE-2019-0657	.NET Framework and Visual Studio Spoofing Vulnerability	Important

.NET Framework	CVE-2019-0613	.NET Framework and Visual Studio Remote Code Execution Vulnerability	Important
Adobe Flash Player	ADV190003	February 2019 Adobe Flash Security Update	Critical
Azure	CVE-2019-0729	Azure IoT Java SDK Privilege Escalation Vulnerability	Important
Azure	CVE-2019-0741	Azure IoT Java SDK Information Disclosure Vulnerbaility	Important
Internet Explorer	CVE-2019-0606	Internet Explorer Memory Corruption Vulnerability	Critical
Internet Explorer	CVE-2019-0676	Internet Explorer Information Disclosure Vulnerability	Important
Microsoft Browsers	CVE-2019-0654	Microsoft Browser Spoofing Vulnerability	Important

Microsoft Edge	CVE-2019-0641	Microsoft Edge Security Feature Bypass Vulnerability	Moderate
Microsoft Edge	CVE-2019-0643	Microsoft Edge Information Disclosure Vulnerability	Moderate
Microsoft Edge	CVE-2019-0645	Microsoft Edge Memory Corruption Vulnerability	Critical
Microsoft Edge	CVE-2019-0650	Microsoft Edge Memory Corruption Vulnerability	Critical
Microsoft Edge	CVE-2019-0634	Microsoft Edge Memory Corruption Vulnerability	Moderate
Microsoft Exchange Server	ADV190004	February 2019 Oracle Outside In Library Security Update	Unknown
Microsoft Exchange Server	CVE-2019-0686	Microsoft Exchange Server Privilege Escalation Vulnerability	Important

Microsoft Exchange Server	CVE-2019-0724	Microsoft Exchange Server Privilege Escalation Vulnerability	Important
Microsoft Exchange Server	ADV190007	Guidance for "PrivExchange" Privilege Escalation Vulnerability	Unknown
Microsoft Graphics Component	CVE-2019-0660	Windows GDI Information Disclosure Vulnerability	Important
Microsoft Graphics Component	CVE-2019-0662	GDI+ Remote Code Execution Vulnerability	Critical
Microsoft Graphics Component	CVE-2019-0664	Windows GDI Information Disclosure Vulnerability	Important
Microsoft Graphics Component	CVE-2019-0602	Windows GDI Information Disclosure Vulnerability	Important
Microsoft Graphics Component	CVE-2019-0615	Windows GDI Information Disclosure Vulnerability	Important
Microsoft Graphics Component	CVE-2019-0616	Windows GDI Information Disclosure Vulnerability	Important

Microsoft Graphics Component	CVE-2019-0618	GDI+ Remote Code Execution Vulnerability	Critical
Microsoft Graphics Component	CVE-2019-0619	Windows GDI Information Disclosure Vulnerability	Important
Microsoft JET Database Engine	CVE-2019-0625	Jet Database Engine Remote Code Execution Vulnerability	Important
Microsoft JET Database Engine	CVE-2019-0595	Jet Database Engine Remote Code Execution Vulnerability	Important
Microsoft JET Database Engine	CVE-2019-0596	Jet Database Engine Remote Code Execution Vulnerability	Important
Microsoft JET Database Engine	CVE-2019-0597	Jet Database Engine Remote Code Execution Vulnerability	Important
Microsoft JET Database Engine	CVE-2019-0598	Jet Database Engine Remote Code Execution Vulnerability	Important

Microsoft JET Database Engine	CVE-2019-0599	Jet Database Engine Remote Code Execution Vulnerability	Important
Microsoft Office	CVE-2019-0540	Microsoft Office Security Feature Bypass Vulnerability	Important
Microsoft Office	CVE-2019-0671	Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability	Important
Microsoft Office	CVE-2019-0672	Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability	Important
Microsoft Office	CVE-2019-0673	Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability	Important
Microsoft Office	CVE-2019-0674	Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability	Important
Microsoft Office	CVE-2019-0675	Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability	Important

Microsoft Office	CVE-2019-0669	Microsoft Excel Information Disclosure Vulnerability	Important
Microsoft Office SharePoint	CVE-2019-0668	Microsoft SharePoint Privilege Escalation Vulnerability	Important
Microsoft Office SharePoint	CVE-2019-0670	Microsoft SharePoint Spoofing Vulnerability	Moderate
Microsoft Office SharePoint	CVE-2019-0594	Microsoft SharePoint Remote Code Execution Vulnerability	Critical
Microsoft Office SharePoint	CVE-2019-0604	Microsoft SharePoint Remote Code Execution Vulnerability	Critical
Microsoft Scripting Engine	CVE-2019-0607	Chakra Scripting Engine Memory Corruption Vulnerability	Critical
Microsoft Scripting Engine	CVE-2019-0610	Chakra Scripting Engine Memory Corruption Vulnerability	Important
Microsoft Scripting Engine	CVE-2019-0640	Chakra Scripting Engine Memory Corruption Vulnerability	Critical

Microsoft Scripting Engine	CVE-2019-0642	Chakra Scripting Engine Memory Corruption Vulnerability	Critical
Microsoft Scripting Engine	CVE-2019-0644	Scripting Engine Memory Corruption Vulnerability	Moderate
Microsoft Scripting Engine	CVE-2019-0648	Scripting Engine Information Disclosure Vulnerability	Important
Microsoft Scripting Engine	CVE-2019-0649	Scripting Engine Elevation of Privileged Vulnerability	Important
Microsoft Scripting Engine	CVE-2019-0651	Scripting Engine Memory Corruption Vulnerability	Critical
Microsoft Scripting Engine	CVE-2019-0652	Scripting Engine Memory Corruption Vulnerability	Critical
Microsoft Scripting Engine	CVE-2019-0655	Scripting Engine Memory Corruption Vulnerability	Moderate
Microsoft Scripting Engine	CVE-2019-0658	Scripting Engine Information Disclosure Vulnerability	Important
Microsoft Scripting Engine	CVE-2019-0590	Chakra Scripting Engine Memory Corruption Vulnerability	Critical

Microsoft Scripting Engine	CVE-2019-0591	Chakra Scripting Engine Memory Corruption Vulnerability	Critical
Microsoft Scripting Engine	CVE-2019-0593	Chakra Scripting Engine Memory Corruption Vulnerability	Critical
Microsoft Scripting Engine	CVE-2019-0605	Chakra Scripting Engine Memory Corruption Vulnerability	Moderate
Microsoft Windows	CVE-2019-0659	Windows Storage Service Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2019-0600	HID Information Disclosure Vulnerability	Important
Microsoft Windows	CVE-2019-0601	HID Information Disclosure Vulnerability	Important
Microsoft Windows	CVE-2019-0627	Windows Security Feature Bypass Vulnerability	Important
Microsoft Windows	CVE-2019-0631	Windows Security Feature Bypass Vulnerability	Important

Microsoft Windows	CVE-2019-0632	Windows Security Feature Bypass Vulnerability	Important
Microsoft Windows	CVE-2019-0636	Windows Information Disclosure Vulnerability	Important
Microsoft Windows	CVE-2019-0637	Windows Defender Firewall Security Feature Bypass Vulnerability	Important
Microsoft Windows	ADV190006	Guidance to mitigate unconstrained delegation vulnerabilities	Unknown
Servicing Stack Updates	ADV990001	Latest Servicing Stack Updates	Critical
Team Foundation Server	CVE-2019-0743	Team Foundation Server Cross-site Scripting Vulnerability	Important
Team Foundation Server	CVE-2019-0742	Team Foundation Server Cross-site Scripting Vulnerability	Important

Visual Studio	CVE-2019-0728	Visual Studio Code Remote Code Execution Vulnerability	Important
Windows DHCP Server	CVE-2019-0626	Windows DHCP Server Remote Code Execution Vulnerability	Critical
Windows Hyper-V	CVE-2019-0635	Windows Hyper-V Information Disclosure Vulnerability	Important
Windows Kernel	CVE-2019-0623	Win32k Privilege Escalation Vulnerability	Important
Windows Kernel	CVE-2019-0628	Win32k Information Disclosure Vulnerability	Important
Windows Kernel	CVE-2019-0656	Windows Kernel Privilege Escalation Vulnerability	Important
Windows Kernel	CVE-2019-0661	Windows Kernel Information Disclosure Vulnerability	Important

Windows Kernel	CVE-2019-0621	Windows Kernel Information Disclosure Vulnerability	Important
Windows SMB Server	CVE-2019-0630	Windows SMB Remote Code Execution Vulnerability	Important
Windows SMB Server	CVE-2019-0633	Windows SMB Remote Code Execution Vulnerability	Important

Recommended Mitigation Measures

Microsoft has released the January 2019 security patch to fix these issues. Please install the patch as soon as possible.

Appendix

ADV190003 - February 2019 Adobe Flash Security Update

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV190003 MITRE NVD	**CVE Title:** February 2019 Adobe Flash Security Update **Description:** This security update addresses the following vulnerability, which is described in Adobe Security Bulletin APSB19-06: CVE-2019-7090. **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 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,	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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. **Mitigations:** **Workarounds:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 5. 6. [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\ActiveX Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}] 7. "Compatibility Flags"=dword:00000400		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 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**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 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:		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	[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: 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**.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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: 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.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 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.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 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		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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**. 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.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

ADV190003						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Adobe Flash Player on Windows Server 2012	4487038 Security Update	Critical	Remote Code Execution	4471331	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV190003						
Adobe Flash Player on Windows 8.1 for 32-bit systems	4487038 Security Update	Critical	Remote Code Execution	4471331	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 8.1 for x64-based systems	4487038 Security Update	Critical	Remote Code Execution	4471331	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows Server 2012 R2	4487038 Security Update	Critical	Remote Code Execution	4471331	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows RT 8.1	4487038 Security Update	Critical	Remote Code Execution	4471331	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 for 32-bit Systems	4487038 Security Update	Critical	Remote Code Execution	4471331	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 for x64-based Systems	4487038 Security Update	Critical	Remote Code Execution	4471331	Base: N/A Temporal:	Yes

ADV190003						
					N/A Vector: N/A	
Adobe Flash Player on Windows Server 2016	4487038 Security Update	Critical	Remote Code Execution	4471331	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1607 for 32-bit Systems	4487038 Security Update	Critical	Remote Code Execution	4471331	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1607 for x64-based Systems	4487038 Security Update	Critical	Remote Code Execution	4471331	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1703 for 32-bit Systems	4487038 Security Update	Critical	Remote Code Execution	4471331	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1703 for x64-based Systems	4487038 Security Update	Critical	Remote Code Execution	4471331	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV190003						
Adobe Flash Player on Windows 10 Version 1709 for 32-bit Systems	4487038 Security Update	Critical	Remote Code Execution	4471331	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1709 for x64-based Systems	4487038 Security Update	Critical	Remote Code Execution	4471331	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1803 for 32-bit Systems	4487038 Security Update	Critical	Remote Code Execution	4471331	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1803 for x64-based Systems	4487038 Security Update	Critical	Remote Code Execution	4471331	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1803 for ARM64-based Systems	4487038 Security Update	Critical	Remote Code Execution	4471331	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1809 for 32-bit Systems	4487038 Security Update	Critical	Remote Code Execution	4471331	Base: N/A Temporal:	Yes

ADV190003						
					N/A Vector: N/A	
Adobe Flash Player on Windows 10 Version 1809 for x64-based Systems	4487038 Security Update	Critical	Remote Code Execution	4471331	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1809 for ARM64-based Systems	4487038 Security Update	Critical	Remote Code Execution	4471331	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows Server 2019	4487038 Security Update	Critical	Remote Code Execution	4471331	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1709 for ARM64-based Systems	4487038 Security Update	Critical	Remote Code Execution	4471331	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV190004 - February 2019 Oracle Outside In Library Security Update

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV190004 MITRE NVD	**CVE Title:** February 2019 Oracle Outside In Library Security Update **Description:** Microsoft Exchange Server contains some elements of the Oracle Outside In libraries. The February 12, 2019 releases of Microsoft Exchange Server contain fixes to vulnerabilities which are described in: • Oracle Critical Patch Update Advisory - October 2018 The following software releases include updates to address the identified vulnerabilities. Product versions or releases that are not listed are past their support life cycle or must be updated to the appropriate February 12, 2019 release of Microsoft Exchange Server to receive the fixes for these vulnerabilities. **FAQ:** None **Mitigations:** None **Workarounds:**	Unknown	Unknown

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

ADV190004						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Exchange Server 2010 Service Pack 3 Update Rollup 26	4487052 Security Update			4468742	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2013 Cumulative Update 22	4345836 Security Update			4468742	Base: N/A Temporal: N/A Vector: N/A	Maybe

ADV190004						
Microsoft Exchange Server 2016 Cumulative Update 12	4471392 Security Update			4468742	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2019 Cumulative Update 1	4471391 Security Update			4468742	Base: N/A Temporal: N/A Vector: N/A	Maybe

ADV190006 - Guidance to mitigate unconstrained delegation vulnerabilities

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV190006 MITRE NVD	**CVE Title:** Guidance to mitigate unconstrained delegation vulnerabilities **Description:**	Unknown	Unknown

Executive Summary

Active Directory Forest trusts provide a secure way for resources in a forest to trust identities from another forest.â€¯This trust is directional;â€¯aâ€¯trusted forest canâ€¯authenticate its users to the trusting forest without allowing the reverse.â€¯

A feature,â€¯*Enforcement for forest boundary for Kerberos full delegation*,â€¯was introduced in Windows Server 2012 that allowsâ€¯anâ€¯administratorâ€¯of the trusted forestâ€¯to configure whetherâ€¯Ticket-Granting Tickets (TGTs) may be delegated toâ€¯a service in a trusting forest.â€¯

An unsafe default configurationâ€¯for this featureâ€¯exists when setting upâ€¯inboundâ€¯trusts that lets an attackerâ€¯in the trusting forestâ€¯requestâ€¯delegation ofâ€¯aâ€¯TGTâ€¯for anâ€¯identityâ€¯fromâ€¯the trusted forest.â€¯

This advisory addresses the issue by recommending a new safe default configurationâ€¯for unconstrained Kerberos delegation across Active Directory forest trustsâ€¯that supersedes the original unsafe configuration.

Recommended Actions

Customers should review Knowledge Base Article 4490425 and take appropriate action.

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The enforcement for forest boundary for Kerberos full delegation will be available as an update for all supported versions of Windows Server starting in the March 2019 Security Update and is currently available for Server 2012 and newer. We recommend that you set the feature on incoming forest trusts. FAQ **1. What is unconstrained delegation?** Unconstrained delegation is when a service can acquire a copy of your TGT to act on your behalf when authenticating to other services. Unconstrained delegation lets the service authenticate to any other service which can lead to security issues such as elevation of privilege. Unconstrained delegation has been replaced by constrained delegation which limits which services can receive tickets on behalf of a user. **2. What is TGT delegation?** TGT delegation allows a service to acquire a TGT from a domain with an inbound trust. This allows any service within an untrusted forest to acquire a TGT to the trusted forest. A feature was introduced in Windows Server 2012 to disable this capability. **3. Why is TGT delegation enabled by default?**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Applications may rely on unconstrained delegation across inbound trusts and disabling delegation may lead to outages. **4. How do I determine if TGT delegation is enabled?** You can check that the flag is set on the trust using PowerShell. Get-AdTrust -filter {TGTDelegation -eq $false} **5. How do I disable TGT delegation?** You can set the EnableTGTDelegation to NO using Netdom. See the KB article for more details. netdom.exe trust fabrikam.com /domain:contoso.com /EnableTGTDelegation:No **6. What is the security risk of leaving TGT delegation enabled?** If an attacker can enable unconstrained delegation of any principal in an untrusted forest and request a service ticket to the trusted forest, they can also request a TGT from the trusted forest. An attacker can then impersonate the user in the trusted forest from within the untrusted forest leading to elevation of privilege. **FAQ:** None **Mitigations:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.1 02/12/2019 08:00:00 In FAQ 4, the PowerShell command has been corrected to: Get-AdTrust -filter {TGTDelegation -eq $false}. This is an informational change only. 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

ADV190006						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1					Base: N/A Temporal:	

ADV190006						
					N/A Vector: N/A	
Windows 7 for x64-based Systems Service Pack 1					Base: N/A Temporal: N/A Vector: N/A	
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)					Base: N/A Temporal: N/A Vector: N/A	
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1					Base: N/A Temporal: N/A Vector: N/A	
Windows Server 2008 R2 for x64-based Systems Service Pack 1					Base: N/A Temporal: N/A Vector: N/A	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)					Base: N/A Temporal: N/A Vector: N/A	

ADV190006						
Windows Server 2012					Base: N/A Temporal: N/A Vector: N/A	
Windows Server 2012 (Server Core installation)					Base: N/A Temporal: N/A Vector: N/A	
Windows 8.1 for 32-bit systems					Base: N/A Temporal: N/A Vector: N/A	
Windows 8.1 for x64-based systems					Base: N/A Temporal: N/A Vector: N/A	
Windows Server 2012 R2					Base: N/A Temporal: N/A Vector: N/A	
Windows RT 8.1					Base: N/A Temporal:	

ADV190006						
					N/A Vector: N/A	
Windows Server 2012 R2 (Server Core installation)					Base: N/A Temporal: N/A Vector: N/A	
Windows 10 for 32-bit Systems					Base: N/A Temporal: N/A Vector: N/A	
Windows 10 for x64-based Systems					Base: N/A Temporal: N/A Vector: N/A	
Windows Server 2016					Base: N/A Temporal: N/A Vector: N/A	
Windows 10 Version 1607 for 32-bit Systems					Base: N/A Temporal: N/A Vector: N/A	

ADV190006						
Windows 10 Version 1607 for x64-based Systems					Base: N/A Temporal: N/A Vector: N/A	
Windows Server 2016 (Server Core installation)					Base: N/A Temporal: N/A Vector: N/A	
Windows 10 Version 1703 for 32-bit Systems					Base: N/A Temporal: N/A Vector: N/A	
Windows 10 Version 1703 for x64-based Systems					Base: N/A Temporal: N/A Vector: N/A	
Windows 10 Version 1709 for 32-bit Systems					Base: N/A Temporal: N/A Vector: N/A	
Windows 10 Version 1709 for x64-based Systems					Base: N/A Temporal:	

ADV190006						
					N/A Vector: N/A	
Windows Server, version 1709 (Server Core Installation)					Base: N/A Temporal: N/A Vector: N/A	
Windows 10 Version 1803 for 32-bit Systems					Base: N/A Temporal: N/A Vector: N/A	
Windows 10 Version 1803 for x64-based Systems					Base: N/A Temporal: N/A Vector: N/A	
Windows Server, version 1803 (Server Core Installation)					Base: N/A Temporal: N/A Vector: N/A	
Windows 10 Version 1803 for ARM64-based Systems					Base: N/A Temporal: N/A Vector: N/A	

ADV190006						
Windows 10 Version 1809 for 32-bit Systems					Base: N/A Temporal: N/A Vector: N/A	
Windows 10 Version 1809 for x64-based Systems					Base: N/A Temporal: N/A Vector: N/A	
Windows 10 Version 1809 for ARM64-based Systems					Base: N/A Temporal: N/A Vector: N/A	
Windows Server 2019					Base: N/A Temporal: N/A Vector: N/A	
Windows Server 2019 (Server Core installation)					Base: N/A Temporal: N/A Vector: N/A	
Windows 10 Version 1709 for ARM64-based Systems					Base: N/A Temporal:	

ADV190006						
					N/A Vector: N/A	
Windows Server 2008 for Itanium-Based Systems Service Pack 2					Base: N/A Temporal: N/A Vector: N/A	
Windows Server 2008 for 32-bit Systems Service Pack 2					Base: N/A Temporal: N/A Vector: N/A	
Windows Server 2008 for x64-based Systems Service Pack 2					Base: N/A Temporal: N/A Vector: N/A	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)					Base: N/A Temporal: N/A Vector: N/A	

ADV190007 - Guidance for "PrivExchange" Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV190007 MITRE NVD	**CVE Title:** Guidance for "PrivExchange" Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Microsoft Exchange Server. An attacker who successfully exploited this vulnerability could attempt to impersonate any other user of the Exchange server. To exploit the vulnerability, an attacker would need to execute a man-in-the-middle attack to forward an authentication request to a Microsoft Exchange Server, thereby allowing impersonation of another Exchange user. To address this vulnerability, a Throttling Policy for EWSMaxSubscriptions could be defined and applied to the organization with a value of zero. This will prevent the Exchange server from sending EWS notifications, and prevent client applications which rely upon EWS notifications from functioning normally. Examples of impacted applications include Outlook for Mac, Skype for Business, notification reliant LOB applications, and some iOS native mail clients. Please see Throttling Policy, for more information. An example:	Unknown	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	New-ThrottlingPolicy -Name AllUsersEWSSubscriptionBlockPolicy -EwsMaxSubscriptions 0 -ThrottlingPolicyScope Organization A planned update is in development. If you determine that your system is at high risk then you should evaluate the proposed workaround. After installing the update you can undo the above action with this command: Remove-ThrottlingPolicy -Identity AllUsersEWSSubscriptionBlockPolicy **FAQ:** **What are the Common Vulnerabilities and Exposures (CVE) identifiers that Microsoft is using to reference this vulnerability?** Microsoft has assigned both CVE-2019-0686 and CVE-2019-0724 to reference the reported vulnerabilities. **Mitigations:** **Workarounds:** One way to prevent EWS from leaking the Exchange server's NTLM credentials is to block EWS subscriptions from being created. This will negatively impact users who rely on EWS clients		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	such as Outlook for Mac, and may also result in unexpected behavior from third-party software that relies on EWS. It may also reduce the number of EWS connections the server can support. Because throttling policies can be applied per user, it is possible to whitelist trusted users who require EWS functionality. **Note**: Customers are strongly encouraged to test workarounds prior to deploying them into production to understand the potential impact. To prevent EWS subscriptions from being created, use the following steps: 1. Create an organization-scoped policy that blocks all EWS subscriptions: 2. `New-ThrottlingPolicy -Name NoEwsSubscriptions -ThrottlingPolicyScope Organization -EwsMaxSubscriptions 0` 3. Create a regular-scoped policy, which can be used to whitelist trusted users who must have full EWS functionality: 4. `New-ThrottlingPolicy -Name AllowEwsSubscriptions -ThrottlingPolicyScope Regular -EwsMaxSubscriptions 5000` 5. Assign the regular policy to any such users: 6. `Set-Mailbox User1 -ThrottlingPolicy AllowEwsSubscriptions` **Note about this EWS Subscription throttling workaround**: A customerâ€™s risk assessment must weigh the protections gained by the workaround as compared to the possible unwanted side		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	effects of the workaround. The following are possible side effects of the EWS Subscription throttling policy: *This workaround may be disruptive to Outlook for Mac, Skype for Business Client, and Apple Mail Clients, causing them to not function properly. Importantly, the throttling policy won't block Autodiscover and Free/Busy requests. The EWS throttling policy will also negatively impact LOB and other third-party Applications that require EWS Notifications. A second policy can be created to whitelist trusted accounts.* **Revision:** 1.1 02/06/2019 08:00:00 Updated vulnerability description to change the command specified to undo the action after installing the update. This is an informational change only. 1.2 02/07/2019 08:00:00 Added FAQ information. This is an informational change only. 1.0 02/05/2019 08:00:00 Information published.		

Affected Software

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

ADV190007						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Exchange Server 2010 Service Pack 3 Update Rollup 26			Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	
Microsoft Exchange Server 2013 Cumulative Update 22			Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	
Microsoft Exchange Server 2016 Cumulative Update 12			Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	
Microsoft Exchange Server 2019 Cumulative Update 1			Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	

ADV990001 - Latest Servicing Stack Updates

<table>
<tr><th>CVE ID</th><th>Vulnerability Description</th><th>Maximum Severity Rating</th><th>Vulnerability Impact</th></tr>
<tr>
<td>ADV990001
MITRE
NVD</td>
<td>
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:
<table>
<tr><th>Product</th><th>SSU Package</th><th>Date Released</th></tr>
<tr><td>Windows Server 2008</td><td>955430</td><td>May 2009</td></tr>
</table>
</td>
<td>Critical</td>
<td>Defense in Depth</td>
</tr>
</table>

CVE ID	Vulnerability Description			Maximum Severity Rating	Vulnerability Impact
	Windows 7/Server 2008 R2	3177467	October 2018		
	Windows Server 2012	3173426	July 2016		
	Windows 8.1/Server 2012 R2	3173424	July 2016		
	Windows 10	4093430	April 2018		
	Windows 10 Version 1607/Server 2016	4485447	February 2019		
	Windows 10 Version 1703	4487327	February 2019		
	Windows 10 1709/Windows Server, version 1709	4485448	February 2019		
	Windows 10 1803/Windows Server, version 1803	4485449	February 2019		
	Windows 10 1809/Server 2019	4470788	December 2018		
	Mitigations: None **Workarounds:** None **Revision:** 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.				

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	2.0 12/05/2018 08:00:00 A Servicing Stack Update has been released for Windows 10 Version 1809 and Windows Server 2019. See the FAQ section for more information. 3.0 12/11/2018 08:00:00 A Servicing Stack Update has been released for Windows 10 Version 1709, Windows Server, version 1709 (Server Core Installation), Windows 10 Version 1803, and Windows Server, version 1803 (Server Core Installation). See the FAQ section for more information. 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. 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. 3.2 12/12/2018 08:00:00 Fixed a typo in the FAQ. 3.1 12/11/2018 08:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Updated supersedence information. This is an informational change only. 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. 1.2 12/03/2018 08:00:00 FAQs have been added to further explain Security Stack Updates. The FAQs include a table that indicates the most recent SSU release for each Windows version. This is an informational change only. 1.0 11/13/2018 08:00:00 Information published.		

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	3177467 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	3177467 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	3177467 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	3177467 Service 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	3177467 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes

ADV990001						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	955430 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012	3173426 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 (Server Core installation)	3173426 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 8.1 for 32-bit systems	3173424 Servicing Stack Update	Critical	Defense in Depth		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		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 R2	3173424 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal:	Yes

ADV990001						
					N/A Vector: N/A	
Windows Server 2012 R2 (Server Core installation)	3173424 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 for 32-bit Systems	4093430 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 for x64-based Systems	4093430 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2016	4485447 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1607 for 32-bit Systems	4485447 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV990001						
Windows 10 Version 1607 for x64-based Systems	4485447 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2016 (Server Core installation)	4485447 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1703 for 32-bit Systems	4487327 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1703 for x64-based Systems	4487327 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for 32-bit Systems	4485448 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for x64-based Systems	4485448 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal:	Yes

ADV990001						
					N/A Vector: N/A	
Windows Server, version 1709 (Server Core Installation)	4485448 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for 32-bit Systems	4485449 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for x64-based Systems	4477137 Servicing Stack Update	Critical	Defense in Depth	4465663	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server, version 1803 (Server Core Installation)	4485449 Servicing Stack Update	Critical	Defense in Depth	4465663	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for ARM64-based Systems	4485449 Servicing Stack Update	Critical	Defense in Depth	4465663	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV990001						
Windows 10 Version 1809 for 32-bit Systems	4470788 Servicing Stack Update	Critical	Defense in Depth	4465664	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1809 for x64-based Systems	4485449 Servicing Stack Update	Critical	Defense in Depth	4465664	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1809 for ARM64-based Systems	4470788 Servicing Stack Update	Critical	Defense in Depth	4465664	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2019	4470788 Servicing Stack Update	Critical	Defense in Depth	4465664	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2019 (Server Core installation)	4470788 Servicing Stack Update	Critical	Defense in Depth	4465664	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for ARM64-based Systems	4485448 Servicing Stack Update	Critical	Defense in Depth	4465664	Base: N/A Temporal:	Yes

ADV990001						
					N/A Vector: N/A	
Windows Server 2008 for Itanium-Based Systems Service Pack 2	955430 Servicing Stack Update	Critical	Defense in Depth	4465664	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	955430 Servicing Stack Update	Critical	Defense in Depth	4465664	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	955430 Servicing Stack Update	Critical	Defense in Depth	4465664	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	955430 Servicing Stack Update	Critical	Defense in Depth	4465664	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0540 - Microsoft Office Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0540 MITRE NVD	**CVE Title:** Microsoft Office Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists when Microsoft Office does not validate URLs. An attacker could send a victim a specially crafted file, which could trick the victim into entering credentials. An attacker who successfully exploited this vulnerability could perform a phishing attack. The update addresses the vulnerability by ensuring Microsoft Office properly validates URLs. **FAQ:** **Does the behavior change after applying this update?** This update causes a change in behavior for documents that have an IncludePicture field with delayed loading for online pictures that are hosted on un-trusted sites that require authentication to load the picture. Before applying the update, a dialog would be displayed requesting that the user authenticate.	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	After applying the update, the picture will not be displayed, and a red X will be shown instead. If the user believes the site is safe, they can add the site into their Trusted Sites through Internet Explorer or Microsoft Edge, and then the online picture can be retrieved. This can only be done if the user knows the name of the site hosting the picture. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0540						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4462174 Security Update	Important	Security Feature Bypass	4461614	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4462174 Security Update	Important	Security Feature Bypass	4461614	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4462138 Security Update	Important	Security Feature Bypass	4461537	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4462138 Security Update	Important	Security Feature Bypass	4461537	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 RT Service Pack 1	4462138 Security Update	Important	Security Feature Bypass	4461537	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0540						
Microsoft Office 2016 (32-bit edition)	4462146 Security Update	Important	Security Feature Bypass	4461535	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	4462146 Security Update	Important	Security Feature Bypass	4461535	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel Viewer	4092465 Security Update	Important	Security Feature Bypass	4022195	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2019 for 32-bit editions	Click to Run Security Update	Important	Security Feature Bypass	4022195	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office 2019 for 64-bit editions	Click to Run Security Update	Important	Security Feature Bypass	4022195	Base: N/A Temporal: N/A Vector: N/A	No
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Security Feature Bypass	4022195	Base: N/A Temporal:	No

CVE-2019-0540						
					N/A Vector: N/A	
Office 365 ProPlus for 64-bit Systems	Click to Run Security Update	Important	Security Feature Bypass	4022195	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office Word Viewer	4462154 Security Update	Important	Security Feature Bypass	4022195	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft PowerPoint Viewer	4092465 Security Update	Important	Security Feature Bypass	4022195	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Compatibility Pack Service Pack 3	4092465 Security Update	Important	Security Feature Bypass	4022195	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0590 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0590 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 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. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0590						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0590						
Microsoft Edge on Windows 10 for 32-bit Systems	4487018 Security Update	Critical	Remote Code Execution	4480962	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	4487018 Security Update	Critical	Remote Code Execution	4480962	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	4487026 Security Update	Moderate	Remote Code Execution	4480961	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	4487026 Security Update	Critical	Remote Code Execution	4480961	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	4487026 Security	Critical	Remote Code Execution	4480961	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0590						
Version 1607 for x64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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-2019-0590						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4486996 Security Update	Critical	Remote Code Execution	4480978	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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-	4487017 Security Update	Critical	Remote Code Execution	4480966	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-2019-0590						
based Systems						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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-2019-0590						
Microsoft Edge on Windows Server 2019	4487044 Security Update	Moderate	Remote Code Execution	4480116	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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	Release Notes Security Update	Critical	Remote Code Execution	4480978	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0591 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0591 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 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. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0591						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0591						
Microsoft Edge on Windows 10 for 32-bit Systems	4487018 Security Update	Critical	Remote Code Execution	4480962	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	4487018 Security Update	Critical	Remote Code Execution	4480962	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	4487026 Security Update	Moderate	Remote Code Execution	4480961	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	4487026 Security Update	Critical	Remote Code Execution	4480961	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	4487026 Security	Critical	Remote Code Execution	4480961	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0591						
Version 1607 for x64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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-2019-0591						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4486996 Security Update	Critical	Remote Code Execution	4480978	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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-	4487017 Security Update	Critical	Remote Code Execution	4480966	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-2019-0591						
based Systems						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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-2019-0591						
Microsoft Edge on Windows Server 2019	4487044 Security Update	Moderate	Remote Code Execution	4480116	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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	Release Notes Security Update	Critical	Remote Code Execution	4480978	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0593 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0593 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 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. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0593						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0593						
Microsoft Edge on Windows 10 for 32-bit Systems	4487018 Security Update	Critical	Remote Code Execution	4480962	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	4487018 Security Update	Critical	Remote Code Execution	4480962	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	4487026 Security Update	Moderate	Remote Code Execution	4480961	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	4487026 Security Update	Critical	Remote Code Execution	4480961	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	4487026 Security	Critical	Remote Code Execution	4480961	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0593						
Version 1607 for x64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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-2019-0593						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4486996 Security Update	Critical	Remote Code Execution	4480978	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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-	4487017 Security Update	Critical	Remote Code Execution	4480966	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-2019-0593						
based Systems						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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-2019-0593						
Microsoft Edge on Windows Server 2019	4487044 Security Update	Moderate	Remote Code Execution	4480116	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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	Release Notes Security Update	Critical	Remote Code Execution	4480978	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0594 - Microsoft SharePoint Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0594 MITRE NVD	**CVE Title:** Microsoft SharePoint Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the SharePoint application pool and the SharePoint server farm account. Exploitation of this vulnerability requires that a user uploads a specially crafted SharePoint application package to an affected versions of SharePoint. The security update addresses the vulnerability by correcting how SharePoint checks the source markup of application packages. **FAQ:** None **Mitigations:** None **Workarounds:** None	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0594						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Server 2010 Service Pack 2	4461630 Security Update	Critical	Remote Code Execution	4461580	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Foundation 2013 Service Pack 1	4462143 Security Update	Critical	Remote Code Execution	4461596	Base: N/A Temporal:	Maybe

CVE-2019-0594						
					N/A Vector: N/A	
Microsoft SharePoint Enterprise Server 2016	4462155 Security Update	Critical	Remote Code Execution	4461598	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Server 2019	4462171 Security Update	Critical	Remote Code Execution	4461634	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0595 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0595 MITRE NVD	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0595						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0595						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487019 Security Only 4487023 Monthly	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0595						
Core installation)	Rollup					
Windows Server 2012	4486993 Security Only 4487025 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4486993 Security Only 4487025 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0595						
Windows 8.1 for x64-based systems	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487000 Monthly Rollup	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4487000 Monthly Rollup 4487028 Security	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0595						
	Only					
Windows 10 for 32-bit Systems	4487018 Security Update	Important	Remote Code Execution	4480962	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487018 Security Update	Important	Remote Code Execution	4480962	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0595						
Windows Server 2016 (Server Core installation)	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487020 Security Update	Important	Remote Code Execution	4480973	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487020 Security Update	Important	Remote Code Execution	4480973	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 1709	4486996 Security	Important	Remote Code Execution	4480978	Base: 7.8 Temporal: 7	Yes

CVE-2019-0595						
(Server Core Installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487044 Security	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7	Yes

CVE-2019-0595						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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-	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0595						
based Systems						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4487023 Monthly Rollup 4487019 Security Only	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487019 Security Only 4487023 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487019 Security Only 4487023 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0595						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4487019 Security Only 4487023 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0596 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0596 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:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0596						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0596						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487019 Security Only 4487023 Monthly	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0596						
Core installation)	Rollup					
Windows Server 2012	4486993 Security Only 4487025 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4486993 Security Only 4487025 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0596						
Windows 8.1 for x64-based systems	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487000 Monthly Rollup	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4487000 Monthly Rollup 4487028 Security	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0596						
	Only					
Windows 10 for 32-bit Systems	4487018 Security Update	Important	Remote Code Execution	4480962	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487018 Security Update	Important	Remote Code Execution	4480962	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0596						
Windows Server 2016 (Server Core installation)	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487020 Security Update	Important	Remote Code Execution	4480973	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487020 Security Update	Important	Remote Code Execution	4480973	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 1709	4486996 Security	Important	Remote Code Execution	4480978	Base: 7.8 Temporal: 7	Yes

CVE-2019-0596						
(Server Core Installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487044 Security	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7	Yes

CVE-2019-0596						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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-	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0596						
based Systems						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4487023 Monthly Rollup 4487019 Security Only	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487019 Security Only 4487023 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487019 Security Only 4487023 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0596						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4487019 Security Only 4487023 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0597 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0597 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:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0597						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0597						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487019 Security Only 4487023 Monthly	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0597						
Core installation)	Rollup					
Windows Server 2012	4486993 Security Only 4487025 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4486993 Security Only 4487025 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0597						
Windows 8.1 for x64-based systems	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487000 Monthly Rollup	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4487000 Monthly Rollup 4487028 Security	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0597						
	Only					
Windows 10 for 32-bit Systems	4487018 Security Update	Important	Remote Code Execution	4480962	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487018 Security Update	Important	Remote Code Execution	4480962	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0597						
Windows Server 2016 (Server Core installation)	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487020 Security Update	Important	Remote Code Execution	4480973	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487020 Security Update	Important	Remote Code Execution	4480973	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 1709	4486996 Security	Important	Remote Code Execution	4480978	Base: 7.8 Temporal: 7	Yes

CVE-2019-0597						
(Server Core Installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487044 Security	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7	Yes

CVE-2019-0597						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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-	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0597						
based Systems						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4487023 Monthly Rollup 4487019 Security Only	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487019 Security Only 4487023 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487019 Security Only 4487023 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0597						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4487019 Security Only 4487023 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0598 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0598 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:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0598						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0598						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487019 Security Only 4487023 Monthly	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0598						
Core installation)	Rollup					
Windows Server 2012	4486993 Security Only 4487025 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4486993 Security Only 4487025 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0598						
Windows 8.1 for x64-based systems	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487000 Monthly Rollup	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4487000 Monthly Rollup 4487028 Security	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0598						
	Only					
Windows 10 for 32-bit Systems	4487018 Security Update	Important	Remote Code Execution	4480962	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487018 Security Update	Important	Remote Code Execution	4480962	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0598						
Windows Server 2016 (Server Core installation)	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487020 Security Update	Important	Remote Code Execution	4480973	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487020 Security Update	Important	Remote Code Execution	4480973	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 1709	4486996 Security	Important	Remote Code Execution	4480978	Base: 7.8 Temporal: 7	Yes

CVE-2019-0598						
(Server Core Installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487044 Security	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7	Yes

CVE-2019-0598						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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-	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0598						
based Systems						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4487023 Monthly Rollup 4487019 Security Only	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487019 Security Only 4487023 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487019 Security Only 4487023 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0598						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4487019 Security Only 4487023 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0599 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0599 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:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0599						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0599						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487019 Security Only 4487023 Monthly	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0599						
Core installation)	Rollup					
Windows Server 2012	4486993 Security Only 4487025 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4486993 Security Only 4487025 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0599						
Windows 8.1 for x64-based systems	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487000 Monthly Rollup	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4487000 Monthly Rollup 4487028 Security	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0599						
	Only					
Windows 10 for 32-bit Systems	4487018 Security Update	Important	Remote Code Execution	4480962	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487018 Security Update	Important	Remote Code Execution	4480962	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0599						
Windows Server 2016 (Server Core installation)	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487020 Security Update	Important	Remote Code Execution	4480973	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487020 Security Update	Important	Remote Code Execution	4480973	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 1709	4486996 Security	Important	Remote Code Execution	4480978	Base: 7.8 Temporal: 7	Yes

CVE-2019-0599						
(Server Core Installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487044 Security	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7	Yes

CVE-2019-0599						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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-	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0599						
based Systems						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4487023 Monthly Rollup 4487019 Security Only	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487019 Security Only 4487023 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487019 Security Only 4487023 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0599						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4487019 Security Only 4487023 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0600 - HID Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0600 MITRE NVD	**CVE Title:** HID Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Human Interface Devices (HID) component improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the victimâ€™s system. To exploit the vulnerability, an attacker would first have to gain execution on the victim system, then run a specially crafted application.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how the HID 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 Kernel memory read - unintentional read access to memory contents in kernel space from a user mode process. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0600						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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	4486563 Monthly	Important	Information Disclosure	4480970	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0600						
R2 for x64-based Systems Service Pack 1 (Server Core installation)	Rollup 4486564 Security Only				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	
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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-2019-0600						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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	4486993 Security Only 4487025 Monthly Rollup	Important	Information Disclosure	4480968	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)	4486993 Security Only 4487025 Monthly Rollup	Important	Information Disclosure	4480968	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-2019-0600						
Windows 8.1 for 32-bit systems	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487000 Monthly	Important	Information Disclosure	4480963	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0600						
	Rollup				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	
Windows Server 2012 R2 (Server Core installation)	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487018 Security Update	Important	Information Disclosure	4480962	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	4487018 Security Update	Important	Information Disclosure	4480962	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	4487026 Security Update	Important	Information Disclosure	4480961	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	4487026 Security	Important	Information Disclosure	4480961	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0600						
1607 for 32-bit Systems	Update				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	
Windows 10 Version 1607 for x64-based Systems	4487026 Security Update	Important	Information Disclosure	4480961	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)	4487026 Security Update	Important	Information Disclosure	4480961	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	4487020 Security Update	Important	Information Disclosure	4480973	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	4487020 Security Update	Important	Information Disclosure	4480973	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	4486996 Security	Important	Information Disclosure	4480978	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0600						
1709 for 32-bit Systems	Update				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	
Windows 10 Version 1709 for x64-based Systems	4486996 Security Update	Important	Information Disclosure	4480978	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 1709 (Server Core Installation)	4486996 Security Update	Important	Information Disclosure	4480978	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	4487017 Security Update	Important	Information Disclosure	4480966	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	4487017 Security Update	Important	Information Disclosure	4480966	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-2019-0600						
Windows Server, version 1803 (Server Core Installation)	4487017 Security Update	Important	Information Disclosure	4480966	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	4487017 Security Update	Important	Information Disclosure	4480966	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	4487044 Security Update	Important	Information Disclosure	4480116	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	4487044 Security Update	Important	Information Disclosure	4480116	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	4487044 Security	Important	Information Disclosure	4480116	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0600						
1809 for ARM64-based Systems	Update				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	
Windows Server 2019	4487044 Security Update	Important	Information Disclosure	4480116	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)	4487044 Security Update	Important	Information Disclosure	4480116	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	4486996 Security Update	Important	Information Disclosure	4480978	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	4487023 Monthly Rollup 4487019 Security	Important	Information Disclosure	4480968	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-2019-0600						
Service Pack 2	Only					
Windows Server 2008 for 32-bit Systems Service Pack 2	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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-2019-0600						
(Server Core installation)						

CVE-2019-0601 - HID Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0601 MITRE NVD	**CVE Title:** HID Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Human Interface Devices (HID) component improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the victimâ€™s 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 HID component handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The type of information that could be disclosed if an attacker successfully exploited this vulnerability is Kernel memory read - unintentional read access to memory contents in kernel space from a user mode process. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0601						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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-2019-0601						
(Server Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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	4487019 Security Only 4487023 Monthly	Important	Information Disclosure	4480968	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-2019-0601						
(Server Core installation)	Rollup					
Windows Server 2012	4486993 Security Only 4487025 Monthly Rollup	Important	Information Disclosure	4480968	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)	4486993 Security Only 4487025 Monthly Rollup	Important	Information Disclosure	4480968	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	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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-2019-0601						
Windows 8.1 for x64-based systems	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487000 Monthly Rollup	Important	Information Disclosure	4480963	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)	4487000 Monthly Rollup 4487028 Security	Important	Information Disclosure	4480963	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-2019-0601						
	Only					
Windows 10 for 32-bit Systems	4487018 Security Update	Important	Information Disclosure	4480962	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	4487018 Security Update	Important	Information Disclosure	4480962	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	4487026 Security Update	Important	Information Disclosure	4480961	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	4487026 Security Update	Important	Information Disclosure	4480961	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	4487026 Security Update	Important	Information Disclosure	4480961	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-2019-0601						
Windows Server 2016 (Server Core installation)	4487026 Security Update	Important	Information Disclosure	4480961	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	4487020 Security Update	Important	Information Disclosure	4480973	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	4487020 Security Update	Important	Information Disclosure	4480973	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	4486996 Security Update	Important	Information Disclosure	4480978	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	4486996 Security Update	Important	Information Disclosure	4480978	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-2019-0601						
Windows Server, version 1709 (Server Core Installation)	4486996 Security Update	Important	Information Disclosure	4480978	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	4487017 Security Update	Important	Information Disclosure	4480966	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	4487017 Security Update	Important	Information Disclosure	4480966	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)	4487017 Security Update	Important	Information Disclosure	4480966	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	4487017 Security	Important	Information Disclosure	4480966	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0601						
1803 for ARM64-based Systems	Update				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	
Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Important	Information Disclosure	4480116	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	4487044 Security Update	Important	Information Disclosure	4480116	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	4487044 Security Update	Important	Information Disclosure	4480116	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	4487044 Security Update	Important	Information Disclosure	4480116	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-2019-0601						
Windows Server 2019 (Server Core installation)	4487044 Security Update	Important	Information Disclosure	4480116	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	4486996 Security Update	Important	Information Disclosure	4480978	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 Service Pack 2	4487023 Monthly Rollup 4487019 Security Only	Important	Information Disclosure	4480968	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	4487019 Security Only 4487023 Monthly	Important	Information Disclosure	4480968	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-2019-0601						
	Rollup					
Windows Server 2008 for x64-based Systems Service Pack 2	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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)	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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-2019-0602 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0602 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 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0602						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems	4486563 Monthly Rollup 4486564	Important	Information Disclosure	4480970	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-2019-0602						
Service Pack 1	Security Only					
Windows 7 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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)	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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-	4486563 Monthly Rollup 4486564	Important	Information Disclosure	4480970	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-2019-0602						
Based Systems Service Pack 1	Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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)	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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	4486993 Security Only 4487025	Important	Information Disclosure	4480968	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-2019-0602						
	Monthly Rollup					
Windows Server 2012 (Server Core installation)	4486993 Security Only 4487025 Monthly Rollup	Important	Information Disclosure	4480968	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	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487000 Monthly Rollup 4487028 Security	Important	Information Disclosure	4480963	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-2019-0602						
	Only					
Windows Server 2012 R2	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487000 Monthly Rollup	Important	Information Disclosure	4480963	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)	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487018 Security	Important	Information Disclosure	4480962	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0602						
	Update				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	
Windows 10 for x64-based Systems	4487018 Security Update	Important	Information Disclosure	4480962	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	4487026 Security Update	Important	Information Disclosure	4480961	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	4487026 Security Update	Important	Information Disclosure	4480961	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	4487026 Security Update	Important	Information Disclosure	4480961	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)	4487026 Security Update	Important	Information Disclosure	4480961	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-2019-0602						
Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Important	Information Disclosure	4480973	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	4487020 Security Update	Important	Information Disclosure	4480973	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	4486996 Security Update	Important	Information Disclosure	4480978	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	4486996 Security Update	Important	Information Disclosure	4480978	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 1709	4486996 Security Update	Important	Information Disclosure	4480978	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-2019-0602						
(Server Core Installation)						
Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Important	Information Disclosure	4480966	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	4487017 Security Update	Important	Information Disclosure	4480966	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)	4487017 Security Update	Important	Information Disclosure	4480966	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	4487017 Security Update	Important	Information Disclosure	4480966	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-2019-0602						
Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Important	Information Disclosure	4480116	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	4487044 Security Update	Important	Information Disclosure	4480116	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	4487044 Security Update	Important	Information Disclosure	4480116	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	4487044 Security Update	Important	Information Disclosure	4480116	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)	4487044 Security Update	Important	Information Disclosure	4480116	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-2019-0602						
Windows 10 Version 1709 for ARM64-based Systems	4486996 Security Update	Important	Information Disclosure	4480978	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 Service Pack 2	4487023 Monthly Rollup 4487019 Security Only	Important	Information Disclosure	4480968	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	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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-	4487019 Security Only	Important	Information Disclosure	4480968	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0602						
based Systems Service Pack 2	4487023 Monthly Rollup				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	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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-2019-0604 - Microsoft SharePoint Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-	**CVE Title:** Microsoft SharePoint Remote Code Execution Vulnerability **Description:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
0604 MITRE NVD	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the SharePoint application pool and the SharePoint server farm account. Exploitation of this vulnerability requires that a user uploads a specially crafted SharePoint application package to an affected versions of SharePoint. The security update addresses the vulnerability by correcting how SharePoint checks the source markup of application packages. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0604						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Server 2010 Service Pack 2	4461630 Security Update	Critical	Remote Code Execution	4461580	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Foundation 2013 Service Pack 1	4462143 Security Update	Critical	Remote Code Execution	4461596	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4462155 Security Update	Critical	Remote Code Execution	4461598	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Server 2019	4462171 Security Update	Critical	Remote Code Execution	4461634	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0605 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0605 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 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. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0605						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0605						
Microsoft Edge on Windows 10 for 32-bit Systems	4487018 Security Update	Critical	Remote Code Execution	4480962	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	4487018 Security Update	Critical	Remote Code Execution	4480962	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	4487026 Security Update	Moderate	Remote Code Execution	4480961	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	4487026 Security Update	Critical	Remote Code Execution	4480961	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	4487026 Security	Critical	Remote Code Execution	4480961	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0605						
Version 1607 for x64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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-2019-0605						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4486996 Security Update	Critical	Remote Code Execution	4480978	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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-	4487017 Security Update	Critical	Remote Code Execution	4480966	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-2019-0605						
based Systems						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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-2019-0605						
Microsoft Edge on Windows Server 2019	4487044 Security Update	Moderate	Remote Code Execution	4480116	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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	Release Notes Security Update	Critical	Remote Code Execution	4480978	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0606 - Internet Explorer Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0606 MITRE NVD	**CVE Title:** Internet Explorer Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, the attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. An attacker could host a specially crafted website designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. The attacker could also take advantage of compromised websites, or websites that accept or host user-provided content or advertisements, by adding specially crafted content that could 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.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by modifying how Internet Explorer handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0606						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4486563 Monthly Rollup 4486474 IE Cumulative	Critical	Remote Code Execution	4480965	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4486474 IE Cumulative 4486563 Monthly Rollup	Critical	Remote Code Execution	4480970	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4486474 IE Cumulative 4486563	Moderate	Remote Code Execution	4480970	Base: 6.4 Temporal: 5.8	Yes

CVE-2019-0606						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	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	
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4486474 IE Cumulative 4487000 Monthly Rollup	Critical	Remote Code Execution	4480963	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4486474 IE Cumulative 4487000 Monthly Rollup	Critical	Remote Code Execution	4480963	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0606						
Internet Explorer 11 on Windows Server 2012 R2	4486474 IE Cumulative 4487000 Monthly Rollup	Moderate	Remote Code Execution	4480963	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	4487000 Monthly Rollup	Critical	Remote Code Execution	4480963	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4487018 Security Update	Critical	Remote Code Execution	4480962	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4487018 Security Update	Critical	Remote Code Execution	4480962	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0606						
x64-based Systems						
Internet Explorer 11 on Windows Server 2016	4487026 Security Update	Moderate	Remote Code Execution	4480961	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	4487026 Security Update	Critical	Remote Code Execution	4480961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4487026 Security Update	Critical	Remote Code Execution	4480961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0606						
x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Critical	Remote Code Execution	4480973	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4487020 Security Update	Critical	Remote Code Execution	4480973	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4486996 Security Update	Critical	Remote Code Execution	4480978	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0606						
1709 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4486996 Security Update	Critical	Remote Code Execution	4480978	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4487017 Security Update	Critical	Remote Code Execution	4480966	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4487017 Security Update	Critical	Remote Code Execution	4480966	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0606						
10 Version 1803 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems	4487017 Security Update	Critical	Remote Code Execution	4480966	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4487044 Security Update	Critical	Remote Code Execution	4480116	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0606						
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Critical	Remote Code Execution	4480116	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems	4487044 Security Update	Critical	Remote Code Execution	4480116	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4487044 Security Update	Moderate	Remote Code Execution	4480116	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-2019-0606						
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems	4486996 Security Update	Critical	Remote Code Execution	4480978	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0607 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0607 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 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

Affected Software

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

CVE-2019-0607						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4486996 Security Update	Critical	Remote Code Execution	4480978	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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-2019-0607						
for x64-based Systems						
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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-2019-0607						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Moderate	Remote Code Execution	4480116	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-2019-0607						
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems	4486996 Security Update	Critical	Remote Code Execution	4480978	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	Release Notes Security Update	Critical	Remote Code Execution	4480978	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-2019-0610 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0610	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A remote code execution vulnerability exists in the way that the 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. 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 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0610						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Important	Remote Code Execution	4480973	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-2019-0610						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4487020 Security Update	Important	Remote Code Execution	4480973	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	4486996 Security Update	Important	Remote Code Execution	4480978	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	4486996 Security Update	Important	Remote Code Execution	4480978	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	4487017 Security	Important	Remote Code Execution	4480966	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0610						
Version 1803 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4487017 Security Update	Important	Remote Code Execution	4480966	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	4487017 Security Update	Important	Remote Code Execution	4480966	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	4487044 Security Update	Important	Remote Code Execution	4480116	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-2019-0610						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Important	Remote Code Execution	4480116	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	4487044 Security Update	Important	Remote Code Execution	4480116	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	4487044 Security Update	Low	Remote Code Execution	4480116	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-	4486996 Security Update	Important	Remote Code Execution	4480978	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-2019-0610						
based Systems						
ChakraCore	Release Notes Security Update	Important	Remote Code Execution	4480978	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0613 - .NET Framework and Visual Studio Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0613 MITRE NVD	**CVE Title:** .NET Framework and Visual Studio Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in .NET Framework and Visual Studio software when the software fails to check the source markup of a file.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of .NET Framework or Visual Studio. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. The security update addresses the vulnerability by correcting how .NET Framework and Visual Studio check the source markup of a file. **FAQ:** None **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0613						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft .NET Framework 4.5.2 on Windows 7 for 32-bit Systems Service Pack 1	4483455 Monthly Rollup 4483474 Security Only	Important	Remote Code Execution	4481481; 4481488	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0613						
Microsoft .NET Framework 4.5.2 on Windows 7 for x64-based Systems Service Pack 1	4483455 Monthly Rollup 4483474 Security Only	Important	Remote Code Execution	4481481; 4481488	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4483455 Monthly Rollup 4483474 Security Only	Important	Remote Code Execution	4481481; 4481488	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4483455 Monthly Rollup 4483474 Security Only	Important	Remote Code Execution	4481481; 4481488	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012	4483454 Monthly Rollup 4483473	Important	Remote Code Execution	4481483; 4481489	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0613						
	Security Only					
Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation)	4483454 Monthly Rollup 4483473 Security Only	Important	Remote Code Execution	4481483; 4481489	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems	4483472 Security Only 4483453 Monthly Rollup	Important	Remote Code Execution	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems	4483472 Security Only 4483453 Monthly Rollup	Important	Remote Code Execution	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2	4483472 Security Only 4483453	Important	Remote Code Execution	4481485; 4481490	Base: N/A Temporal: N/A	Maybe

CVE-2019-0613						
	Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows RT 8.1	4483453 Monthly Rollup	Important	Remote Code Execution	4481484; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation)	4483472 Security Only 4483453 Monthly Rollup	Important	Remote Code Execution	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4483474 Security Only 4483455 Monthly Rollup	Important	Remote Code Execution	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for x64-based Systems Service Pack 2	4483474 Security Only 4483455	Important	Remote Code Execution	4481485; 4481490	Base: N/A Temporal: N/A	Maybe

CVE-2019-0613						
	Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2	4483470 Security Only 4483451 Monthly Rollup	Important	Remote Code Execution	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6 on Windows Server 2008 for x64-based Systems Service Pack 2	4483470 Security Only 4483451 Monthly Rollup	Important	Remote Code Execution	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Visual Studio 2017	Release Notes Security Update	Important	Remote Code Execution	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for 32-bit Systems	4487017 Security	Important	Remote Code Execution	4480966	Base: N/A Temporal: N/A	Yes

CVE-2019-0613						
	Update				Vector: N/A	
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for x64-based Systems	4487017 Security Update	Important	Remote Code Execution	4480966	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.2 on Windows Server, version 1803 (Server Core Installation)	4487017 Security Update	Important	Remote Code Execution	4480966	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for ARM64-based Systems	4487017 Security Update	Important	Remote Code Execution	4480966	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1809 for 32-bit Systems	4483452 Monthly Rollup	Important	Remote Code Execution	4480056; 4481031	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0613						
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1809 for x64-based Systems	4483452 Monthly Rollup	Important	Remote Code Execution	4480056; 4481031	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.2 on Windows Server 2019	4483452 Monthly Rollup	Important	Remote Code Execution	4480056; 4481031	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.2 on Windows Server 2019 (Server Core installation)	4483452 Monthly Rollup	Important	Remote Code Execution	4480056; 4481031	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6/4.6.1/4.6.2 on Windows 10 for 32-bit Systems	4487018 Security Update	Important	Remote Code Execution	4480962	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6/4.6.1/4.6.2 on Windows 10 for x64-based Systems	4487018 Security	Important	Remote Code Execution	4480962	Base: N/A Temporal: N/A	Yes

CVE-2019-0613						
	Update				Vector: N/A	
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for 32-bit Systems Service Pack 1	4483451 Monthly Rollup 4483474 Security Only	Important	Remote Code Execution	4481481; 4481488	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for x64-based Systems Service Pack 1	4483451 Monthly Rollup 4483470 Security Only	Important	Remote Code Execution	4481481; 4481488	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4483451 Monthly Rollup 4483470 Security Only	Important	Remote Code Execution	4481481; 4481488	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4483451 Monthly Rollup	Important	Remote Code Execution	4481481; 4481488	Base: N/A Temporal: N/A	Maybe

CVE-2019-0613						
	4483470 Security Only				Vector: N/A	
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012	4483449 Monthly Rollup 4483468 Security Only	Important	Remote Code Execution	4481483; 4481489	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 (Server Core installation)	4483449 Monthly Rollup 4483468 Security Only	Important	Remote Code Execution	4481483; 4481489	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for 32-bit systems	4483469 Security Only 4483450 Monthly Rollup	Important	Remote Code Execution	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for x64-based systems	4483469 Security Only	Important	Remote Code Execution	4481485; 4481490	Base: N/A Temporal:	Maybe

CVE-2019-0613						
	4483450 Monthly Rollup				N/A Vector: N/A	
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2	4483469 Security Only 4483450 Monthly Rollup	Important	Remote Code Execution	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows RT 8.1	4483450 Monthly Rollup	Important	Remote Code Execution	4481484; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2 (Server Core installation)	4483469 Security Only 4483450 Monthly Rollup	Important	Remote Code Execution	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016	4487026 Security	Important	Remote Code Execution	4480961	Base: N/A Temporal:	Yes

CVE-2019-0613						
	Update				N/A Vector: N/A	
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for 32-bit Systems	4487026 Security Update	Important	Remote Code Execution	4480961	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for x64-based Systems	4487026 Security Update	Important	Remote Code Execution	4480961	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016 (Server Core installation)	4487026 Security Update	Important	Remote Code Execution	4480961	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7/4.7.1/4.7.2 on Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Important	Remote Code Execution	4480973	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0613						
Microsoft .NET Framework 4.7/4.7.1/4.7.2 on Windows 10 Version 1703 for x64-based Systems	4487020 Security Update	Important	Remote Code Execution	4480973	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.1/4.7.2 on Windows 10 Version 1709 for 32-bit Systems	4486996 Security Update	Important	Remote Code Execution	4480978	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.1/4.7.2 on Windows 10 Version 1709 for x64-based Systems	4486996 Security Update	Important	Remote Code Execution	4480978	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.1/4.7.2 on Windows Server, version 1709 (Server Core Installation)	4486996 Security Update	Important	Remote Code Execution	4480978	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.1/4.7.2 on Windows 10 Version 1709 for ARM64-based Systems	4486996 Security	Important	Remote Code Execution	4480978	Base: N/A Temporal: N/A	Yes

CVE-2019-0613						
	Update				Vector: N/A	
Microsoft Visual Studio 2017 version 15.9	Release Notes Security Update	Important	Remote Code Execution	4480978	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012	4483456 Monthly Rollup 4483481 Security Only	Important	Remote Code Execution	4481483; 4481489	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation)	4483456 Monthly Rollup 4483481 Security Only	Important	Remote Code Execution	4481483; 4481489	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems	4483484 Security Only 4483459 Monthly	Important	Remote Code Execution	4481485; 4481490	Base: N/A Temporal: N/A	Maybe

CVE-2019-0613						
	Rollup				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems	4483484 Security Only 4483459 Monthly Rollup	Important	Remote Code Execution	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2	4483484 Security Only 4483459 Monthly Rollup	Important	Remote Code Execution	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation)	4483484 Security Only 4483459 Monthly Rollup	Important	Remote Code Execution	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 10 for 32-bit Systems	4487018 Security	Important	Remote Code Execution	4480962	Base: N/A Temporal: N/A	Yes

CVE-2019-0613						
	Update				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows 10 for x64-based Systems	4487018 Security Update	Important	Remote Code Execution	4480962	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server 2016	4487026 Security Update	Important	Remote Code Execution	4480961	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for 32-bit Systems	4487026 Security Update	Important	Remote Code Execution	4480961	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for x64-based Systems	4487026 Security Update	Important	Remote Code Execution	4480961	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0613						
Microsoft .NET Framework 3.5 on Windows Server 2016 (Server Core installation)	4487026 Security Update	Important	Remote Code Execution	4480961	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Important	Remote Code Execution	4480973	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for x64-based Systems	4487020 Security Update	Important	Remote Code Execution	4480973	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for 32-bit Systems	4486996 Security Update	Important	Remote Code Execution	4480978	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for x64-based Systems	4486996 Security	Important	Remote Code Execution	4480978	Base: N/A Temporal: N/A	Yes

CVE-2019-0613						
	Update				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows Server, version 1709 (Server Core Installation)	4486996 Security Update	Important	Remote Code Execution	4480978	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Important	Remote Code Execution	4480966	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for x64-based Systems	4487017 Security Update	Important	Remote Code Execution	4480966	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server, version 1803 (Server Core Installation)	4487017 Security Update	Important	Remote Code Execution	4480966	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0613						
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for ARM64-based Systems	4487017 Security Update	Important	Remote Code Execution	4480966	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1809 for 32-bit Systems	4483452 Monthly Rollup	Important	Remote Code Execution	4480056; 4481031	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1809 for x64-based Systems	4483452 Monthly Rollup	Important	Remote Code Execution	4480056; 4481031	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server 2019	4483452 Monthly Rollup	Important	Remote Code Execution	4480056; 4481031	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server 2019 (Server Core installation)	4483452 Monthly	Important	Remote Code Execution	4480056; 4481031	Base: N/A Temporal: N/A	Yes

CVE-2019-0613						
	Rollup				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for ARM64-based Systems	4486996 Security Update	Important	Remote Code Execution	4480978	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2	4483482 Security Only 4483457 Monthly Rollup	Important	Remote Code Execution	4467227; 4481487	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4483482 Security Only 4483457 Monthly Rollup	Important	Remote Code Execution	4481487; 4481491	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2	4483482 Security Only 4483457 Monthly	Important	Remote Code Execution	4481487; 4481491	Base: N/A Temporal: N/A	Maybe

CVE-2019-0613						
	Rollup				Vector: N/A	
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4483482 Security Only 4483457 Monthly Rollup	Important	Remote Code Execution	4481487; 4481491	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2	4483482 Security Only 4483457 Monthly Rollup	Important	Remote Code Execution	4481487; 4481491	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows 7 for 32-bit Systems Service Pack 1	4483458 Monthly Rollup 4483483 Security Only	Important	Remote Code Execution	4481481; 4481488	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows 7 for x64-based Systems Service Pack 1	4483458 Monthly Rollup	Important	Remote Code Execution	4481481; 4481488	Base: N/A Temporal: N/A	Maybe

CVE-2019-0613						
	4483483 Security Only				Vector: N/A	
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4483458 Monthly Rollup 4483483 Security Only	Important	Remote Code Execution	4481481; 4481488	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4483458 Monthly Rollup 4483483 Security Only	Important	Remote Code Execution	4467224; 4481481	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4483458 Monthly Rollup 4483483 Security Only	Important	Remote Code Execution	4481481; 4481488	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0615 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0615 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 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0615						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems	4486563 Monthly Rollup 4486564	Important	Information Disclosure	4480970	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-2019-0615						
Service Pack 1	Security Only					
Windows 7 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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)	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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-	4486563 Monthly Rollup 4486564	Important	Information Disclosure	4480970	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-2019-0615						
Based Systems Service Pack 1	Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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)	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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	4486993 Security Only 4487025	Important	Information Disclosure	4480968	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-2019-0615						
	Monthly Rollup					
Windows Server 2012 (Server Core installation)	4486993 Security Only 4487025 Monthly Rollup	Important	Information Disclosure	4480968	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	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487000 Monthly Rollup 4487028 Security	Important	Information Disclosure	4480963	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-2019-0615						
	Only					
Windows Server 2012 R2	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487000 Monthly Rollup	Important	Information Disclosure	4480963	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)	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487018 Security	Important	Information Disclosure	4480962	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0615						
	Update				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	
Windows 10 for x64-based Systems	4487018 Security Update	Important	Information Disclosure	4480962	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	4487026 Security Update	Important	Information Disclosure	4480961	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	4487026 Security Update	Important	Information Disclosure	4480961	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	4487026 Security Update	Important	Information Disclosure	4480961	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)	4487026 Security Update	Important	Information Disclosure	4480961	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-2019-0615						
Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Important	Information Disclosure	4480973	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	4487020 Security Update	Important	Information Disclosure	4480973	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	4486996 Security Update	Important	Information Disclosure	4480978	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	4486996 Security Update	Important	Information Disclosure	4480978	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 1709	4486996 Security Update	Important	Information Disclosure	4480978	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-2019-0615						
(Server Core Installation)						
Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Important	Information Disclosure	4480966	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	4487017 Security Update	Important	Information Disclosure	4480966	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)	4487017 Security Update	Important	Information Disclosure	4480966	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	4487017 Security Update	Important	Information Disclosure	4480966	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-2019-0615						
Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Important	Information Disclosure	4480116	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	4487044 Security Update	Important	Information Disclosure	4480116	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	4487044 Security Update	Important	Information Disclosure	4480116	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	4487044 Security Update	Important	Information Disclosure	4480116	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)	4487044 Security Update	Important	Information Disclosure	4480116	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-2019-0615						
Windows 10 Version 1709 for ARM64-based Systems	4486996 Security Update	Important	Information Disclosure	4480978	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 Service Pack 2	4487023 Monthly Rollup 4487019 Security Only	Important	Information Disclosure	4480968	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	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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-	4487019 Security Only	Important	Information Disclosure	4480968	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0615						
based Systems Service Pack 2	4487023 Monthly Rollup				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	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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-2019-0616 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0616	**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:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0616						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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-2019-0616						
Windows 7 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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)	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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-2019-0616						
Service Pack 1						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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)	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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	4486993 Security Only 4487025 Monthly	Important	Information Disclosure	4480968	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-2019-0616						
	Rollup					
Windows Server 2012 (Server Core installation)	4486993 Security Only 4487025 Monthly Rollup	Important	Information Disclosure	4480968	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	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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-2019-0616						
Windows Server 2012 R2	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487000 Monthly Rollup	Important	Information Disclosure	4480963	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)	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487018 Security Update	Important	Information Disclosure	4480962	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-2019-0616						
Windows 10 for x64-based Systems	4487018 Security Update	Important	Information Disclosure	4480962	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	4487026 Security Update	Important	Information Disclosure	4480961	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	4487026 Security Update	Important	Information Disclosure	4480961	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	4487026 Security Update	Important	Information Disclosure	4480961	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)	4487026 Security Update	Important	Information Disclosure	4480961	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	4487020 Security	Important	Information Disclosure	4480973	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0616						
1703 for 32-bit Systems	Update				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	
Windows 10 Version 1703 for x64-based Systems	4487020 Security Update	Important	Information Disclosure	4480973	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	4486996 Security Update	Important	Information Disclosure	4480978	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	4486996 Security Update	Important	Information Disclosure	4480978	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 1709 (Server Core Installation)	4486996 Security Update	Important	Information Disclosure	4480978	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-2019-0616						
Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Important	Information Disclosure	4480966	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	4487017 Security Update	Important	Information Disclosure	4480966	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)	4487017 Security Update	Important	Information Disclosure	4480966	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	4487017 Security Update	Important	Information Disclosure	4480966	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	4487044 Security	Important	Information Disclosure	4480116	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0616						
1809 for 32-bit Systems	Update				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	
Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Important	Information Disclosure	4480116	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	4487044 Security Update	Important	Information Disclosure	4480116	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	4487044 Security Update	Important	Information Disclosure	4480116	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)	4487044 Security Update	Important	Information Disclosure	4480116	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	4486996 Security	Important	Information Disclosure	4480978	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0616						
1709 for ARM64-based Systems	Update				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	
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4487023 Monthly Rollup 4487019 Security Only	Important	Information Disclosure	4480968	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	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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	4487019 Security Only 4487023 Monthly	Important	Information Disclosure	4480968	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-2019-0616						
Service Pack 2	Rollup					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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-2019-0618 - GDI+ Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0618	**CVE Title:** GDI+ Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory. An attacker who successfully exploited this	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. There are multiple ways an attacker could exploit the vulnerability: • In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability and then convince users to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to open an email attachment or click a link in an email or instant message. • In a file-sharing attack scenario, an attacker could provide a specially crafted document file that is designed to exploit the vulnerability, and then convince users to open the document file. The security update addresses the vulnerability by correcting the way that the Windows GDI handles objects in the memory. **FAQ:** None **Mitigations:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0618						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems	4486563 Monthly Rollup 4486564	Critical	Remote Code Execution	4480970	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-2019-0618						
Service Pack 1	Security Only					
Windows 7 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Critical	Remote Code Execution	4480970	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)	4486563 Monthly Rollup 4486564 Security Only	Critical	Remote Code Execution	4480970	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-	4486563 Monthly Rollup 4486564	Critical	Remote Code Execution	4480970	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-2019-0618						
Based Systems Service Pack 1	Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Critical	Remote Code Execution	4480970	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)	4487019 Security Only 4487023 Monthly Rollup	Critical	Remote Code Execution	4480968	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	4486993 Security Only 4487025	Critical	Remote Code Execution	4480968	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-2019-0618						
	Monthly Rollup					
Windows Server 2012 (Server Core installation)	4486993 Security Only 4487025 Monthly Rollup	Critical	Remote Code Execution	4480968	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	4487000 Monthly Rollup 4487028 Security Only	Critical	Remote Code Execution	4480963	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	4487000 Monthly Rollup 4487028 Security	Critical	Remote Code Execution	4480963	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-2019-0618						
	Only					
Windows Server 2012 R2	4487000 Monthly Rollup 4487028 Security Only	Critical	Remote Code Execution	4480963	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 RT 8.1	4487000 Monthly Rollup	Critical	Remote Code Execution	4480963	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)	4487000 Monthly Rollup 4487028 Security Only	Critical	Remote Code Execution	4480963	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	4487018 Security	Critical	Remote Code Execution	4480962	Base: 8.8 Temporal: 7.9	Yes

CVE-2019-0618						
	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 for x64-based Systems	4487018 Security Update	Critical	Remote Code Execution	4480962	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	4487026 Security Update	Critical	Remote Code Execution	4480961	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4487026 Security Update	Critical	Remote Code Execution	4480961	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	4487026 Security Update	Critical	Remote Code Execution	4480961	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)	4487026 Security Update	Critical	Remote Code Execution	4480961	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-2019-0618						
Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4487020 Security Update	Critical	Remote Code Execution	4480973	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4486996 Security Update	Critical	Remote Code Execution	4480978	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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 1709 (Server Core Installation)	4486996 Security Update	Critical	Remote Code Execution	4480978	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-2019-0618						
Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487017 Security Update	Critical	Remote Code Execution	4480966	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4487017 Security Update	Critical	Remote Code Execution	4480966	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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-2019-0618						
Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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)	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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-2019-0618						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4487023 Monthly Rollup 4487019 Security Only	Critical	Remote Code Execution	4480968	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	4487019 Security Only 4487023 Monthly Rollup	Critical	Remote Code Execution	4480968	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	4487019 Security Only 4487023 Monthly Rollup	Critical	Remote Code Execution	4480968	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-2019-0618						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4487019 Security Only 4487023 Monthly Rollup	Critical	Remote Code Execution	4480968	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-2019-0619 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0619 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.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0619						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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	4486563 Monthly	Important	Information Disclosure	4480970	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0619						
R2 for x64-based Systems Service Pack 1 (Server Core installation)	Rollup 4486564 Security Only				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	
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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-2019-0619						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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	4486993 Security Only 4487025 Monthly Rollup	Important	Information Disclosure	4480968	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)	4486993 Security Only 4487025 Monthly Rollup	Important	Information Disclosure	4480968	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-2019-0619						
Windows 8.1 for 32-bit systems	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487000 Monthly	Important	Information Disclosure	4480963	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0619						
	Rollup				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	
Windows Server 2012 R2 (Server Core installation)	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487018 Security Update	Important	Information Disclosure	4480962	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	4487018 Security Update	Important	Information Disclosure	4480962	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	4487026 Security Update	Important	Information Disclosure	4480961	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	4487026 Security	Important	Information Disclosure	4480961	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0619						
1607 for 32-bit Systems	Update				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	
Windows 10 Version 1607 for x64-based Systems	4487026 Security Update	Important	Information Disclosure	4480961	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)	4487026 Security Update	Important	Information Disclosure	4480961	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	4487020 Security Update	Important	Information Disclosure	4480973	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	4487020 Security Update	Important	Information Disclosure	4480973	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	4486996 Security	Important	Information Disclosure	4480978	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0619						
1709 for 32-bit Systems	Update				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	
Windows 10 Version 1709 for x64-based Systems	4486996 Security Update	Important	Information Disclosure	4480978	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 1709 (Server Core Installation)	4486996 Security Update	Important	Information Disclosure	4480978	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	4487017 Security Update	Important	Information Disclosure	4480966	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	4487017 Security Update	Important	Information Disclosure	4480966	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-2019-0619						
Windows Server, version 1803 (Server Core Installation)	4487017 Security Update	Important	Information Disclosure	4480966	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	4487017 Security Update	Important	Information Disclosure	4480966	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	4487044 Security Update	Important	Information Disclosure	4480116	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	4487044 Security Update	Important	Information Disclosure	4480116	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	4487044 Security	Important	Information Disclosure	4480116	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0619						
1809 for ARM64-based Systems	Update				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	
Windows Server 2019	4487044 Security Update	Important	Information Disclosure	4480116	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)	4487044 Security Update	Important	Information Disclosure	4480116	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	4486996 Security Update	Important	Information Disclosure	4480978	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	4487023 Monthly Rollup 4487019 Security	Important	Information Disclosure	4480968	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-2019-0619						
Service Pack 2	Only					
Windows Server 2008 for 32-bit Systems Service Pack 2	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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-2019-0619						
(Server Core installation)						

CVE-2019-0621 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0621 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system. The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory.	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 Kernel memory read - unintentional read access to memory contents in kernel space from a user mode process. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0621						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4486563 Monthly	Important	Information Disclosure	4480970	Base: 5.5 Temporal: 5	Yes

CVE-2019-0621						
R2 for x64-based Systems Service Pack 1 (Server Core installation)	Rollup 4486564 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0621						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4486993 Security Only 4487025 Monthly Rollup	Important	Information Disclosure	4480968	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4486993 Security Only 4487025 Monthly Rollup	Important	Information Disclosure	4480968	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0621						
Windows 8.1 for 32-bit systems	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4487000 Monthly	Important	Information Disclosure	4480963	Base: 5.5 Temporal: 5	Yes

CVE-2019-0621						
	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 2012 R2 (Server Core installation)	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4487018 Security Update	Important	Information Disclosure	4480962	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4487018 Security Update	Important	Information Disclosure	4480962	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4487026 Security Update	Important	Information Disclosure	4480961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4487026 Security	Important	Information Disclosure	4480961	Base: 5.5 Temporal: 5	Yes

CVE-2019-0621						
1607 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1607 for x64-based Systems	4487026 Security Update	Important	Information Disclosure	4480961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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)	4487026 Security Update	Important	Information Disclosure	4480961	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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 1703 for 32-bit Systems	4487020 Security Update	Important	Information Disclosure	4480973	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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 1703 for x64-based Systems	4487020 Security Update	Important	Information Disclosure	4480973	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4486996 Security	Important	Information Disclosure	4480978	Base: 5.5 Temporal: 5	Yes

CVE-2019-0621						
1709 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1709 for x64-based Systems	4486996 Security Update	Important	Information Disclosure	4480978	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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 1709 (Server Core Installation)	4486996 Security Update	Important	Information Disclosure	4480978	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4487017 Security Update	Important	Information Disclosure	4480966	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4487017 Security Update	Important	Information Disclosure	4480966	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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,	4487017 Security	Important	Information Disclosure	4480966	Base: 5.5 Temporal: 5	Yes

CVE-2019-0621						
version 1803 (Server Core Installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1803 for ARM64-based Systems	4487017 Security Update	Important	Information Disclosure	4480966	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Important	Information Disclosure	4480116	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Important	Information Disclosure	4480116	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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-	4487044 Security Update	Important	Information Disclosure	4480116	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0621						
based Systems						
Windows Server 2019	4487044 Security Update	Important	Information Disclosure	4480116	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4487044 Security Update	Important	Information Disclosure	4480116	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4486996 Security Update	Important	Information Disclosure	4480978	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4487023 Monthly Rollup 4487019 Security Only	Important	Information Disclosure	4480968	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0621						
Windows Server 2008 for 32-bit Systems Service Pack 2	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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)	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0623 - Win32k Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0623 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:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0623						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Elevation of Privilege	4480970	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0623						
Windows 7 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Elevation of Privilege	4480970	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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)	4486563 Monthly Rollup 4486564 Security Only	Important	Elevation of Privilege	4480970	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4486563 Monthly Rollup 4486564 Security Only	Important	Elevation of Privilege	4480970	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0623						
Service Pack 1						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Elevation of Privilege	4480970	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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)	4487019 Security Only 4487023 Monthly Rollup	Important	Elevation of Privilege	4480968	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4486993 Security Only 4487025 Monthly	Important	Elevation of Privilege	4480968	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0623						
	Rollup					
Windows Server 2012 (Server Core installation)	4486993 Security Only 4487025 Monthly Rollup	Important	Elevation of Privilege	4480968	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4487000 Monthly Rollup 4487028 Security Only	Important	Elevation of Privilege	4480963	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4487000 Monthly Rollup 4487028 Security Only	Important	Elevation of Privilege	4480963	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0623						
Windows Server 2012 R2	4487000 Monthly Rollup 4487028 Security Only	Important	Elevation of Privilege	4480963	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4487000 Monthly Rollup	Important	Elevation of Privilege	4480963	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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)	4487000 Monthly Rollup 4487028 Security Only	Important	Elevation of Privilege	4480963	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4487018 Security Update	Important	Elevation of Privilege	4480962	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0623						
Windows 10 for x64-based Systems	4487018 Security Update	Important	Elevation of Privilege	4480962	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4487026 Security Update	Important	Elevation of Privilege	4480961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4487026 Security Update	Important	Elevation of Privilege	4480961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4487026 Security Update	Important	Elevation of Privilege	4480961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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)	4487026 Security Update	Important	Elevation of Privilege	4480961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4487020 Security	Important	Elevation of Privilege	4480973	Base: 7 Temporal: 6.3	Yes

CVE-2019-0623						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1703 for x64-based Systems	4487020 Security Update	Important	Elevation of Privilege	4480973	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4486996 Security Update	Important	Elevation of Privilege	4480978	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4486996 Security Update	Important	Elevation of Privilege	4480978	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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 1709 (Server Core Installation)	4486996 Security Update	Important	Elevation of Privilege	4480978	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4487017 Security Update	Important	Elevation of Privilege	4480966	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0623						
Windows 10 Version 1803 for x64-based Systems	4487017 Security Update	Important	Elevation of Privilege	4480966	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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)	4487017 Security Update	Important	Elevation of Privilege	4480966	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4487017 Security Update	Important	Elevation of Privilege	4480966	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for ARM64-based Systems	4486996 Security Update	Important	Elevation of Privilege	4480978	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4487023 Monthly Rollup 4487019	Important	Elevation of Privilege	4480968	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0623						
Systems Service Pack 2	Security Only					
Windows Server 2008 for 32-bit Systems Service Pack 2	4487019 Security Only 4487023 Monthly Rollup	Important	Elevation of Privilege	4480968	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4487019 Security Only 4487023 Monthly Rollup	Important	Elevation of Privilege	4480968	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4487019 Security Only 4487023 Monthly	Important	Elevation of Privilege	4480968	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0623						
Core installation)	Rollup					

CVE-2019-0625 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0625 MITRE NVD	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** None **Mitigations:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0625						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0625						
	Only					
Windows 7 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486563 Monthly Rollup 4486564 Security	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0625						
Systems Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4487019 Security Only 4487023 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486993 Security Only 4487025 Monthly	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0625						
	Rollup					
Windows Server 2012 (Server Core installation)	4486993 Security Only 4487025 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0625						
Windows Server 2012 R2	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487000 Monthly Rollup	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487018 Security Update	Important	Remote Code Execution	4480962	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0625						
Windows 10 for x64-based Systems	4487018 Security Update	Important	Remote Code Execution	4480962	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487020 Security	Important	Remote Code Execution	4480973	Base: 7.8 Temporal: 7	Yes

CVE-2019-0625						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1703 for x64-based Systems	4487020 Security Update	Important	Remote Code Execution	4480973	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 1709 (Server Core Installation)	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0625						
Windows 10 Version 1803 for x64-based Systems	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0625						
Windows 10 Version 1809 for ARM64-based Systems	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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)	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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 Itanium-Based Systems	4487023 Monthly Rollup 4487019 Security	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0625						
Service Pack 2	Only					
Windows Server 2008 for 32-bit Systems Service Pack 2	4487019 Security Only 4487023 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487019 Security Only 4487023 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/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	4487019 Security Only 4487023 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0625						
Core installation)						

CVE-2019-0626 - Windows DHCP Server Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0626 MITRE NVD	**CVE Title:** Windows DHCP Server Remote Code Execution Vulnerability **Description:** A memory corruption vulnerability exists in the Windows Server DHCP service when an attacker sends specially crafted packets to a DHCP server. An attacker who successfully exploited the vulnerability could run arbitrary code on the DHCP server. To exploit the vulnerability, an attacker could send a specially crafted packet to a DHCP server. The security update addresses the vulnerability by correcting how DHCP servers handle network packets. **FAQ:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0626						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems	4486563 Monthly Rollup	Critical	Remote Code Execution	4480970	Base: 9.8 Temporal: 8.8	Yes

CVE-2019-0626						
Service Pack 1	4486564 Security Only				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 7 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Critical	Remote Code Execution	4480970	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4486563 Monthly Rollup 4486564 Security Only	Critical	Remote Code Execution	4480970	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for	4486563 Monthly Rollup	Critical	Remote Code Execution	4480970	Base: 9.8 Temporal: 8.8	Yes

CVE-2019-0626						
Itanium-Based Systems Service Pack 1	4486564 Security Only				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Critical	Remote Code Execution	4480970	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4487019 Security Only 4487023 Monthly Rollup	Critical	Remote Code Execution	4480968	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4486993 Security Only	Critical	Remote Code Execution	4480968	Base: 9.8 Temporal: 8.8	Yes

CVE-2019-0626						
	4487025 Monthly Rollup				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2012 (Server Core installation)	4486993 Security Only 4487025 Monthly Rollup	Critical	Remote Code Execution	4480968	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4487000 Monthly Rollup 4487028 Security Only	Critical	Remote Code Execution	4480963	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4487000 Monthly Rollup 4487028 Security	Critical	Remote Code Execution	4480963	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0626						
	Only					
Windows Server 2012 R2	4487000 Monthly Rollup 4487028 Security Only	Critical	Remote Code Execution	4480963	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4487000 Monthly Rollup	Critical	Remote Code Execution	4480963	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4487000 Monthly Rollup 4487028 Security Only	Critical	Remote Code Execution	4480963	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4487018 Security	Critical	Remote Code Execution	4480962	Base: 9.8 Temporal: 8.8	Yes

CVE-2019-0626						
	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 for x64-based Systems	4487018 Security Update	Critical	Remote Code Execution	4480962	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4487026 Security Update	Critical	Remote Code Execution	4480961	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4487026 Security Update	Critical	Remote Code Execution	4480961	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4487026 Security Update	Critical	Remote Code Execution	4480961	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4487026 Security Update	Critical	Remote Code Execution	4480961	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0626						
Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Critical	Remote Code Execution	4480973	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4487020 Security Update	Critical	Remote Code Execution	4480973	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4486996 Security Update	Critical	Remote Code Execution	4480978	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4486996 Security Update	Critical	Remote Code Execution	4480978	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4486996 Security Update	Critical	Remote Code Execution	4480978	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0626						
Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Critical	Remote Code Execution	4480966	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4487017 Security Update	Critical	Remote Code Execution	4480966	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4487017 Security Update	Critical	Remote Code Execution	4480966	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4487017 Security Update	Critical	Remote Code Execution	4480966	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Critical	Remote Code Execution	4480116	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0626						
Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Critical	Remote Code Execution	4480116	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4487044 Security Update	Critical	Remote Code Execution	4480116	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4487044 Security Update	Critical	Remote Code Execution	4480116	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4487044 Security Update	Critical	Remote Code Execution	4480116	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4486996 Security Update	Critical	Remote Code Execution	4480978	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0626						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4487023 Monthly Rollup 4487019 Security Only	Critical	Remote Code Execution	4480968	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4487019 Security Only 4487023 Monthly Rollup	Critical	Remote Code Execution	4480968	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4487019 Security Only 4487023 Monthly Rollup	Critical	Remote Code Execution	4480968	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0626						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4487019 Security Only 4487023 Monthly Rollup	Critical	Remote Code Execution	4480968	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0627 - Windows Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0627 MITRE NVD	**CVE Title:** Windows Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard. An attacker who successfully exploited this vulnerability could circumvent a User Mode Code Integrity (UMCI) policy on the machine. To exploit the vulnerability, an attacker would first have to access the local machine, and then run a malicious program.	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The update addresses the vulnerability by correcting how Windows validates User Mode Code Integrity policies. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0627						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4487018 Security Update	Important	Security Feature Bypass	4480962	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 for x64-based Systems	4487018 Security Update	Important	Security Feature Bypass	4480962	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 2016	4487026 Security Update	Important	Security Feature Bypass	4480961	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 1607 for 32-bit Systems	4487026 Security Update	Important	Security Feature Bypass	4480961	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 1607 for x64-based Systems	4487026 Security Update	Important	Security Feature Bypass	4480961	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-2019-0627						
Windows Server 2016 (Server Core installation)	4487026 Security Update	Important	Security Feature Bypass	4480961	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 1703 for 32-bit Systems	4487020 Security Update	Important	Security Feature Bypass	4480973	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 1703 for x64-based Systems	4487020 Security Update	Important	Security Feature Bypass	4480973	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 1709 for 32-bit Systems	4486996 Security Update	Important	Security Feature Bypass	4480978	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 1709 for x64-based Systems	4486996 Security Update	Important	Security Feature Bypass	4480978	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, version 1709	4486996 Security	Important	Security Feature Bypass	4480978	Base: 5.3 Temporal: 4.8	Yes

CVE-2019-0627						
(Server Core Installation)	Update				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	
Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Important	Security Feature Bypass	4480966	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 1803 for x64-based Systems	4487017 Security Update	Important	Security Feature Bypass	4480966	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, version 1803 (Server Core Installation)	4487017 Security Update	Important	Security Feature Bypass	4480966	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 1803 for ARM64-based Systems	4487017 Security Update	Important	Security Feature Bypass	4480966	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 32-bit Systems	4487044 Security Update	Important	Security Feature Bypass	4480116	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-2019-0627						
Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Important	Security Feature Bypass	4480116	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 ARM64-based Systems	4487044 Security Update	Important	Security Feature Bypass	4480116	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	4487044 Security Update	Important	Security Feature Bypass	4480116	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)	4487044 Security Update	Important	Security Feature Bypass	4480116	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 1709 for ARM64-based Systems	4486996 Security Update	Important	Security Feature Bypass	4480978	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-2019-0628 - Win32k Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0628 MITRE NVD	**CVE Title:** Win32k Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the win32k component improperly provides kernel information. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how win32k handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory. **Mitigations:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0628						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security	Important	Information Disclosure	4480970	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-2019-0628						
	Only					
Windows 7 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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)	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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	4486563 Monthly Rollup 4486564 Security	Important	Information Disclosure	4480970	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-2019-0628						
Systems Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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)	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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	4486993 Security Only 4487025 Monthly	Important	Information Disclosure	4480968	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-2019-0628						
	Rollup					
Windows Server 2012 (Server Core installation)	4486993 Security Only 4487025 Monthly Rollup	Important	Information Disclosure	4480968	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	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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-2019-0628						
Windows Server 2012 R2	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487000 Monthly Rollup	Important	Information Disclosure	4480963	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)	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487018 Security Update	Important	Information Disclosure	4480962	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-2019-0628						
Windows 10 for x64-based Systems	4487018 Security Update	Important	Information Disclosure	4480962	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	4487026 Security Update	Important	Information Disclosure	4480961	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	4487026 Security Update	Important	Information Disclosure	4480961	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	4487026 Security Update	Important	Information Disclosure	4480961	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)	4487026 Security Update	Important	Information Disclosure	4480961	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	4487020 Security	Important	Information Disclosure	4480973	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0628						
1703 for 32-bit Systems	Update				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	
Windows 10 Version 1703 for x64-based Systems	4487020 Security Update	Important	Information Disclosure	4480973	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	4486996 Security Update	Important	Information Disclosure	4480978	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	4486996 Security Update	Important	Information Disclosure	4480978	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 1709 (Server Core Installation)	4486996 Security Update	Important	Information Disclosure	4480978	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-2019-0628						
Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Important	Information Disclosure	4480966	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	4487017 Security Update	Important	Information Disclosure	4480966	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)	4487017 Security Update	Important	Information Disclosure	4480966	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	4487017 Security Update	Important	Information Disclosure	4480966	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	4487044 Security	Important	Information Disclosure	4480116	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0628						
1809 for 32-bit Systems	Update				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	
Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Important	Information Disclosure	4480116	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	4487044 Security Update	Important	Information Disclosure	4480116	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	4487044 Security Update	Important	Information Disclosure	4480116	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)	4487044 Security Update	Important	Information Disclosure	4480116	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	4486996 Security	Important	Information Disclosure	4480978	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0628						
1709 for ARM64-based Systems	Update				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	
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4487023 Monthly Rollup 4487019 Security Only	Important	Information Disclosure	4480968	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	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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	4487019 Security Only 4487023 Monthly	Important	Information Disclosure	4480968	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-2019-0628						
Service Pack 2	Rollup					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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-2019-0630 - Windows SMB Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0630 MITRE NVD	**CVE Title:** Windows SMB Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests. An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, in most situations, an authenticated attacker could send a specially crafted packet to a targeted SMBv2 server. The security update addresses the vulnerability by correcting how SMBv2 handles these specially crafted requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0630						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0630						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4486563 Monthly Rollup 4486564 Security Only	Important	Remote Code Execution	4480970	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4487019 Security Only 4487023 Monthly	Important	Remote Code Execution	4480968	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0630						
Core installation)	Rollup					
Windows Server 2012	4486993 Security Only 4487025 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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)	4486993 Security Only 4487025 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0630						
Windows 8.1 for x64-based systems	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4487000 Monthly Rollup	Important	Remote Code Execution	4480963	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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)	4487000 Monthly Rollup 4487028 Security	Important	Remote Code Execution	4480963	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0630						
	Only					
Windows 10 for 32-bit Systems	4487018 Security Update	Important	Remote Code Execution	4480962	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4487018 Security Update	Important	Remote Code Execution	4480962	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0630						
Windows Server 2016 (Server Core installation)	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4487020 Security Update	Important	Remote Code Execution	4480973	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4487020 Security Update	Important	Remote Code Execution	4480973	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0630						
Windows Server, version 1709 (Server Core Installation)	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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)	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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-	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0630						
based Systems						
Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4487044 Security	Important	Remote Code Execution	4480116	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0630						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1709 for ARM64-based Systems	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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 Service Pack 2	4487023 Monthly Rollup 4487019 Security Only	Important	Remote Code Execution	4480968	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4487019 Security Only 4487023 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0630						
Windows Server 2008 for x64-based Systems Service Pack 2	4487019 Security Only 4487023 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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)	4487019 Security Only 4487023 Monthly Rollup	Important	Remote Code Execution	4480968	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0631 - Windows Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0631 MITRE NVD	**CVE Title:** Windows Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard. An attacker who successfully exploited this vulnerability could circumvent a User Mode Code Integrity (UMCI) policy on the machine. To exploit the vulnerability, an attacker would first have to access the local machine, and then run a malicious program. The update addresses the vulnerability by correcting how Windows validates User Mode Code Integrity policies. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00	Important	Security Feature Bypass

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

Affected Software

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

CVE-2019-0631						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4487018 Security Update	Important	Security Feature Bypass	4480962	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 for x64-based Systems	4487018 Security Update	Important	Security Feature Bypass	4480962	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-2019-0631						
Windows Server 2016	4487026 Security Update	Important	Security Feature Bypass	4480961	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 1607 for 32-bit Systems	4487026 Security Update	Important	Security Feature Bypass	4480961	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 1607 for x64-based Systems	4487026 Security Update	Important	Security Feature Bypass	4480961	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 2016 (Server Core installation)	4487026 Security Update	Important	Security Feature Bypass	4480961	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 1703 for 32-bit Systems	4487020 Security Update	Important	Security Feature Bypass	4480973	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 1703	4487020 Security	Important	Security Feature Bypass	4480973	Base: 5.3 Temporal: 4.8	Yes

CVE-2019-0631						
for x64-based Systems	Update				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	
Windows 10 Version 1709 for 32-bit Systems	4486996 Security Update	Important	Security Feature Bypass	4480978	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 1709 for x64-based Systems	4486996 Security Update	Important	Security Feature Bypass	4480978	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, version 1709 (Server Core Installation)	4486996 Security Update	Important	Security Feature Bypass	4480978	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 1803 for 32-bit Systems	4487017 Security Update	Important	Security Feature Bypass	4480966	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 1803 for x64-based Systems	4487017 Security Update	Important	Security Feature Bypass	4480966	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-2019-0631						
Windows Server, version 1803 (Server Core Installation)	4487017 Security Update	Important	Security Feature Bypass	4480966	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 1803 for ARM64-based Systems	4487017 Security Update	Important	Security Feature Bypass	4480966	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 32-bit Systems	4487044 Security Update	Important	Security Feature Bypass	4480116	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-based Systems	4487044 Security Update	Important	Security Feature Bypass	4480116	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 ARM64-based Systems	4487044 Security Update	Important	Security Feature Bypass	4480116	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-2019-0631						
Windows Server 2019	4487044 Security Update	Important	Security Feature Bypass	4480116	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)	4487044 Security Update	Important	Security Feature Bypass	4480116	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 1709 for ARM64-based Systems	4486996 Security Update	Important	Security Feature Bypass	4480978	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-2019-0632 - Windows Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0632	**CVE Title:** 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 in Windows which could allow an attacker to bypass Device Guard. An attacker who successfully exploited this vulnerability could circumvent a User Mode Code Integrity (UMCI) policy on the machine. To exploit the vulnerability, an attacker would first have to access the local machine, and then run a malicious program. The update addresses the vulnerability by correcting how Windows validates User Mode Code Integrity policies. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0632						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4487018 Security Update	Important	Security Feature Bypass	4480962	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 for x64-based Systems	4487018 Security Update	Important	Security Feature Bypass	4480962	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 2016	4487026 Security Update	Important	Security Feature Bypass	4480961	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 1607 for 32-bit Systems	4487026 Security Update	Important	Security Feature Bypass	4480961	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-2019-0632						
Windows 10 Version 1607 for x64-based Systems	4487026 Security Update	Important	Security Feature Bypass	4480961	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 2016 (Server Core installation)	4487026 Security Update	Important	Security Feature Bypass	4480961	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 1703 for 32-bit Systems	4487020 Security Update	Important	Security Feature Bypass	4480973	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 1703 for x64-based Systems	4487020 Security Update	Important	Security Feature Bypass	4480973	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 1709 for 32-bit Systems	4486996 Security Update	Important	Security Feature Bypass	4480978	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 1709	4486996 Security	Important	Security Feature Bypass	4480978	Base: 5.3 Temporal: 4.8	Yes

CVE-2019-0632						
for x64-based Systems	Update				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	
Windows Server, version 1709 (Server Core Installation)	4486996 Security Update	Important	Security Feature Bypass	4480978	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 1803 for 32-bit Systems	4487017 Security Update	Important	Security Feature Bypass	4480966	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 1803 for x64-based Systems	4487017 Security Update	Important	Security Feature Bypass	4480966	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, version 1803 (Server Core Installation)	4487017 Security Update	Important	Security Feature Bypass	4480966	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 1803	4487017 Security	Important	Security Feature Bypass	4480966	Base: 5.3 Temporal: 4.8	Yes

CVE-2019-0632						
for ARM64-based Systems	Update				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	
Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Important	Security Feature Bypass	4480116	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-based Systems	4487044 Security Update	Important	Security Feature Bypass	4480116	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 ARM64-based Systems	4487044 Security Update	Important	Security Feature Bypass	4480116	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	4487044 Security Update	Important	Security Feature Bypass	4480116	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)	4487044 Security Update	Important	Security Feature Bypass	4480116	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-2019-0632						
Windows 10 Version 1709 for ARM64-based Systems	4486996 Security Update	Important	Security Feature Bypass	4480978	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-2019-0633 - Windows SMB Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0633 MITRE NVD	**CVE Title:** Windows SMB Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests. An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server. To exploit the vulnerability, in most situations, an authenticated attacker could send a specially crafted packet to a targeted SMBv2 server. The security update addresses the vulnerability by correcting how SMBv2 handles these specially crafted requests. **FAQ:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0633						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012	4486993 Security Only	Important	Remote Code Execution		Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0633						
	4487025 Monthly Rollup				Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2012 (Server Core installation)	4486993 Security Only 4487025 Monthly Rollup	Important	Remote Code Execution		Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4487000 Monthly Rollup 4487028 Security	Important	Remote Code Execution	4480963	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0633						
	Only					
Windows Server 2012 R2	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4487000 Monthly Rollup	Important	Remote Code Execution	4480963	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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)	4487000 Monthly Rollup 4487028 Security Only	Important	Remote Code Execution	4480963	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4487018 Security	Important	Remote Code Execution	4480962	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0633						
	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 for x64-based Systems	4487018 Security Update	Important	Remote Code Execution	4480962	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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)	4487026 Security Update	Important	Remote Code Execution	4480961	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0633						
Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Important	Remote Code Execution	4480973	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4487020 Security Update	Important	Remote Code Execution	4480973	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0633						
Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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)	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4487017 Security Update	Important	Remote Code Execution	4480966	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version	4487044 Security	Important	Remote Code Execution	4480116	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0633						
1809 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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)	4487044 Security Update	Important	Remote Code Execution	4480116	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0633						
Windows 10 Version 1709 for ARM64-based Systems	4486996 Security Update	Important	Remote Code Execution	4480978	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0634 - Microsoft Edge Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0634 MITRE NVD	**CVE Title:** Microsoft Edge Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that enables an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 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 by way of enticement in an email or Instant Messenger message, or by getting them to open an attachment sent through email. The security update addresses the vulnerability by modifying how Microsoft Edge handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

Affected Software

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

CVE-2019-0634						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4487020 Security Update	Critical	Remote Code Execution	4480973	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-2019-0634						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4486996 Security Update	Critical	Remote Code Execution	4480978	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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-2019-0634						
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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-2019-0634						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Moderate	Remote Code Execution	4480116	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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-2019-0634						
1709 for ARM64-based Systems						

CVE-2019-0635 - Windows Hyper-V Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0635 MITRE NVD	**CVE Title:** Windows Hyper-V Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system. To exploit the vulnerability, an attacker on a guest operating system could run a specially crafted application that could cause the Hyper-V host operating system to disclose memory information. An attacker who successfully exploited the vulnerability could gain access to information on the Hyper-V host operating system. The security update addresses the vulnerability by correcting how Hyper-V validates guest operating system user input.	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 Kernel memory read - unintentional read access to memory contents in kernel space from a user mode process. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0635						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0635						
Core installation)						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4486993 Security Only 4487025 Monthly Rollup	Important	Information Disclosure	4480970	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4486993 Security Only 4487025 Monthly Rollup	Important	Information Disclosure	4480970	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0635						
Windows 8.1 for x64-based systems	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-	4487018 Security	Important	Information Disclosure	4480962	Base: 5.4 Temporal: 4.9	Yes

CVE-2019-0635						
based Systems	Update				Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2016	4487026 Security Update	Important	Information Disclosure	4480961	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4487026 Security Update	Important	Information Disclosure	4480961	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4487026 Security Update	Important	Information Disclosure	4480961	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4487020 Security Update	Important	Information Disclosure	4480973	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version	4486996 Security	Important	Information Disclosure	4480978	Base: 5.4 Temporal: 4.9	Yes

CVE-2019-0635						
1709 for x64-based Systems	Update				Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server, version 1709 (Server Core Installation)	4486996 Security Update	Important	Information Disclosure	4480978	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4487017 Security Update	Important	Information Disclosure	4480966	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4487017 Security Update	Important	Information Disclosure	4480966	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0635						
Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Important	Information Disclosure	4480116	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4487044 Security Update	Important	Information Disclosure	4480116	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4487044 Security Update	Important	Information Disclosure	4480116	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	Base: 5.4 Temporal: 4.9 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008	4487019 Security	Important	Information Disclosure	4480968	Base: 5.4 Temporal: 4.9	Yes

CVE-2019-0635						
for x64-based Systems Service Pack 2 (Server Core installation)	Only 4487023 Monthly Rollup				Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C	

CVE-2019-0636 - Windows Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0636 MITRE NVD	**CVE Title:** Windows Information Disclosure Vulnerability **Description:** An information vulnerability exists when Windows improperly discloses file information. Successful exploitation of the vulnerability could allow the attacker to read the contents of files on disk. To exploit the vulnerability, an attacker would have to log onto an affected system and run a specially crafted application.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The update addresses the vulnerability by changing the way Windows discloses file information. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is unauthorized file system access - reading from file system. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0636						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2008	4486563 Monthly	Important	Information Disclosure	4480970	Base: 5.5 Temporal: 5.1	Yes

CVE-2019-0636						
R2 for x64-based Systems Service Pack 1 (Server Core installation)	Rollup 4486564 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes

CVE-2019-0636						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2012	4486993 Security Only 4487025 Monthly Rollup	Important	Information Disclosure	4480968	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4486993 Security Only 4487025 Monthly Rollup	Important	Information Disclosure	4480968	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes

CVE-2019-0636						
Windows 8.1 for 32-bit systems	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2012 R2	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows RT 8.1	4487000 Monthly	Important	Information Disclosure	4480963	Base: 5.5 Temporal: 5.1	Yes

CVE-2019-0636						
	Rollup				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	
Windows Server 2012 R2 (Server Core installation)	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4487018 Security Update	Important	Information Disclosure	4480962	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4487018 Security Update	Important	Information Disclosure	4480962	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2016	4487026 Security Update	Important	Information Disclosure	4480961	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version	4487026 Security	Important	Information Disclosure	4480961	Base: 5.5 Temporal: 5.1	Yes

CVE-2019-0636						
1607 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	
Windows 10 Version 1607 for x64-based Systems	4487026 Security Update	Important	Information Disclosure	4480961	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4487026 Security Update	Important	Information Disclosure	4480961	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Important	Information Disclosure	4480973	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4487020 Security Update	Important	Information Disclosure	4480973	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version	4486996 Security	Important	Information Disclosure	4480978	Base: 5.5 Temporal: 5.1	Yes

CVE-2019-0636						
1709 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	
Windows 10 Version 1709 for x64-based Systems	4486996 Security Update	Important	Information Disclosure	4480978	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4486996 Security Update	Important	Information Disclosure	4480978	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Important	Information Disclosure	4480966	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4487017 Security Update	Important	Information Disclosure	4480966	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows Server,	4487017 Security	Important	Information Disclosure	4480966	Base: 5.5 Temporal: 5.1	Yes

CVE-2019-0636						
version 1803 (Server Core Installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	
Windows 10 Version 1803 for ARM64-based Systems	4487017 Security Update	Important	Information Disclosure	4480966	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Important	Information Disclosure	4480116	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Important	Information Disclosure	4480116	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-	4487044 Security Update	Important	Information Disclosure	4480116	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes

CVE-2019-0636						
based Systems						
Windows Server 2019	4487044 Security Update	Important	Information Disclosure	4480116	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4487044 Security Update	Important	Information Disclosure	4480116	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4486996 Security Update	Important	Information Disclosure	4480978	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4487023 Monthly Rollup 4487019 Security Only	Important	Information Disclosure	4480968	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes

CVE-2019-0636						
Windows Server 2008 for 32-bit Systems Service Pack 2	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	Base: 5.5 Temporal: 5.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes

CVE-2019-0637 - Windows Defender Firewall Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0637 MITRE NVD	**CVE Title:** Windows Defender Firewall Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists when Windows Defender Firewall incorrectly applies firewall profiles to cellular network connections. This vulnerability occurs when Windows is connected to both an ethernet network and a cellular network. An attacker would have no way to trigger this vulnerability remotely, and this vulnerability by itself does not allow Windows to be exploited. This update addresses the behavior by correcting how Windows Defender Firewall handles firewall profiles when ethernet and cellular network connections are both present. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0637						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1709 for 32-bit Systems	4486996 Security Update	Important	Security Feature Bypass	4480978	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709	4486996 Security	Important	Security Feature Bypass	4480978	Base: 5.3 Temporal: 4.8	Yes

CVE-2019-0637						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	
Windows Server, version 1709 (Server Core Installation)	4486996 Security Update	Important	Security Feature Bypass	4480978	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Important	Security Feature Bypass	4480966	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4487017 Security Update	Important	Security Feature Bypass	4480966	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4487017 Security Update	Important	Security Feature Bypass	4480966	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-	4487017 Security	Important	Security Feature Bypass	4480966	Base: 5.3 Temporal: 4.8	Yes

CVE-2019-0637						
based Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Important	Security Feature Bypass	4480116	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Important	Security Feature Bypass	4480116	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4487044 Security Update	Important	Security Feature Bypass	4480116	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4487044 Security Update	Important	Security Feature Bypass	4480116	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4487044 Security Update	Important	Security Feature Bypass	4480116	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0637						
Windows 10 Version 1709 for ARM64-based Systems	4486996 Security Update	Important	Security Feature Bypass	4480978	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0640 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0640 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 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.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0640						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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-2019-0640						
for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4486996 Security Update	Critical	Remote Code Execution	4480978	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487017 Security	Critical	Remote Code Execution	4480966	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0640						
Version 1803 for ARM64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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-2019-0640						
Microsoft Edge on Windows Server 2019	4487044 Security Update	Moderate	Remote Code Execution	4480116	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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	Release Notes Security Update	Critical	Remote Code Execution	4480978	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-2019-0641 - Microsoft Edge Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0641 MITRE NVD	**CVE Title:** Microsoft Edge Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists in Microsoft Edge handles whitelisting. Edge depends on a default whitelist of sites where Adobe Flash will load without user interaction. Because the whitelist was not scheme-aware, an attacker could use a man in the middle attack to cause Flash policies to be bypassed and arbitrary Flash content to be loaded without user interaction. The security update addresses the vulnerability by modifying how affected Microsoft Edge handles whitelisting. **FAQ:** None **Mitigations:** None **Workarounds:** None	Moderate	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0641						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Moderate	Security Feature Bypass	4480973	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0641						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4487020 Security Update	Moderate	Security Feature Bypass	4480973	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4486996 Security Update	Moderate	Security Feature Bypass	4480978	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4486996 Security Update	Moderate	Security Feature Bypass	4480978	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803	4487017 Security Update	Moderate	Security Feature Bypass	4480966	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0641						
for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4487017 Security Update	Moderate	Security Feature Bypass	4480966	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4487017 Security Update	Moderate	Security Feature Bypass	4480966	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Moderate	Security Feature Bypass	4480116	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0641						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Moderate	Security Feature Bypass	4480116	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4487044 Security Update	Moderate	Security Feature Bypass	4480116	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2019	4487044 Security Update	Low	Security Feature Bypass	4480116	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Edge on Windows 10 Version 1709 for ARM64-	4486996 Security Update	Moderate	Security Feature Bypass	4480978	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0641						
based Systems						

CVE-2019-0642 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0642 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 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0642						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4487018 Security Update	Critical	Remote Code Execution	4480962	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	4487018 Security Update	Critical	Remote Code Execution	4480962	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	4487026 Security Update	Moderate	Remote Code Execution	4480961	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	4487026 Security Update	Critical	Remote Code Execution	4480961	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-2019-0642						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4487026 Security Update	Critical	Remote Code Execution	4480961	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	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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-2019-0642						
for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4486996 Security Update	Critical	Remote Code Execution	4480978	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487017 Security	Critical	Remote Code Execution	4480966	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0642						
Version 1803 for ARM64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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-2019-0642						
Microsoft Edge on Windows Server 2019	4487044 Security Update	Moderate	Remote Code Execution	4480116	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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	Release Notes Security Update	Critical	Remote Code Execution	4480978	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0643 - Microsoft Edge Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0643 MITRE NVD	**CVE Title:** Microsoft Edge Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the way that Microsoft Edge handles cross-origin requests. An attacker who successfully exploited this vulnerability could determine the origin of all webpages in the affected browser. In a web-based attack scenario, an attacker could host a website that is used to attempt to exploit the vulnerability. Additionally, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could be used to exploit the vulnerability. However, in all cases an attacker would have no way to force users to view attacker-controlled content. Instead, an attacker would have to convince users to take action. For example, an attacker could trick users into clicking a link that takes them to the attacker's site. The security update addresses the vulnerability by correcting how Microsoft Edge handles cross-origin requests. **FAQ:** **What type of information could be disclosed by this vulnerability?**	Moderate	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The type of information that could be disclosed if an attacker successfully exploited this vulnerability is unauthorized file system access - reading from file system. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0643						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Moderate	Information Disclosure	4480116	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/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Moderate	Information Disclosure	4480116	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/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-	4487044 Security Update	Moderate	Information Disclosure	4480116	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/RC:C	Yes

CVE-2019-0643						
based Systems						
Microsoft Edge on Windows Server 2019	4487044 Security Update	Low	Information Disclosure	4480116	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/RC:C	Yes

CVE-2019-0644 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0644 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 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	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0644						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows Server 2016	4487026 Security Update	Moderate	Remote Code Execution	4480961	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	4487026 Security Update	Critical	Remote Code Execution	4480961	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	4487026 Security Update	Critical	Remote Code Execution	4480961	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-2019-0644						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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-2019-0644						
for x64-based Systems						
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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-2019-0644						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Moderate	Remote Code Execution	4480116	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-2019-0644						
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems	4486996 Security Update	Critical	Remote Code Execution	4480978	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	Release Notes Security Update	Critical	Remote Code Execution	4480978	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-2019-0645 - Microsoft Edge Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0645	**CVE Title:** Microsoft Edge Memory Corruption Vulnerability **Description:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that enables an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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 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 by way of enticement in an email or Instant Messenger message, or by getting them to open an attachment sent through email. The security update addresses the vulnerability by modifying how Microsoft Edge handles objects in memory. **FAQ:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0645						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10	4487018 Security	Critical	Remote Code Execution	4480962	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0645						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 for x64-based Systems	4487018 Security Update	Critical	Remote Code Execution	4480962	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	4487026 Security Update	Moderate	Remote Code Execution	4480961	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	4487026 Security Update	Critical	Remote Code Execution	4480961	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	4487026 Security Update	Critical	Remote Code Execution	4480961	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-2019-0645						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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-2019-0645						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4486996 Security Update	Critical	Remote Code Execution	4480978	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487017 Security	Critical	Remote Code Execution	4480966	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0645						
Version 1803 for ARM64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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-2019-0645						
ARM64-based Systems						
Microsoft Edge on Windows Server 2019	4487044 Security Update	Moderate	Remote Code Execution	4480116	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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-2019-0648 - Scripting Engine Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0648 MITRE NVD	**CVE Title:** Scripting Engine Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Chakra improperly discloses the contents of its memory, which could provide an attacker with information to further compromise the userâ€™s computer or data. To exploit the vulnerability, an attacker must know the memory address of where the object was created. The update addresses the vulnerability by changing the way certain functions handle objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory. **Mitigations:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0648						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1809 for	4487044 Security Update	Important	Information Disclosure	4480116	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/RC:C	Yes

CVE-2019-0648						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Important	Information Disclosure	4480116	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/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4487044 Security Update	Important	Information Disclosure	4480116	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/RC:C	Yes
Microsoft Edge on Windows Server 2019	4487044 Security Update	Low	Information Disclosure	4480116	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/RC:C	Yes

CVE-2019-0649 - Scripting Engine Elevation of Privileged Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0649 MITRE NVD	**CVE Title:** Scripting Engine Elevation of Privileged Vulnerability **Description:** A vulnerability exists in Microsoft Chakra JIT server. An attacker who successfully exploited this vulnerability could gain elevated privileges. The vulnerability by itself does not allow arbitrary code to run. However, this vulnerability could be used in conjunction with one or more vulnerabilities (for example a remote code execution vulnerability and another elevation of privilege vulnerability) to take advantage of the elevated privileges when running. The security update addresses the vulnerability by modifying how Microsoft Chakra handles constructorCaches. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0649						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Important	Elevation of Privilege	4480973	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-2019-0649						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4487020 Security Update	Important	Elevation of Privilege	4480973	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	4486996 Security Update	Important	Elevation of Privilege	4480978	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	4486996 Security Update	Important	Elevation of Privilege	4480978	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	4487017 Security Update	Important	Elevation of Privilege	4480966	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-2019-0649						
for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4487017 Security Update	Important	Elevation of Privilege	4480966	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	4487017 Security Update	Important	Elevation of Privilege	4480966	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	4487044 Security Update	Important	Elevation of Privilege	4480116	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-2019-0649						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Important	Elevation of Privilege	4480116	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	4487044 Security Update	Important	Elevation of Privilege	4480116	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	4487044 Security Update	Low	Elevation of Privilege	4480116	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-	4486996 Security Update	Important	Elevation of Privilege	4480978	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-2019-0649						
based Systems						
ChakraCore	Release Notes Security Update	Important	Elevation of Privilege	4480978	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-2019-0650 - Microsoft Edge Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0650 MITRE NVD	**CVE Title:** Microsoft Edge Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that enables an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. An	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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 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 by way of enticement in an email or Instant Messenger message, or by getting them to open an attachment sent through email. The security update addresses the vulnerability by modifying how Microsoft Edge handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0650						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Critical	Remote Code Execution	4480966	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-2019-0650						
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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-2019-0650						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Moderate	Remote Code Execution	4480116	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-2019-0651 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0651 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 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. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0651						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0651						
Microsoft Edge on Windows 10 for 32-bit Systems	4487018 Security Update	Critical	Remote Code Execution	4480962	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	4487018 Security Update	Critical	Remote Code Execution	4480962	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	4487026 Security Update	Moderate	Remote Code Execution	4480961	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	4487026 Security Update	Critical	Remote Code Execution	4480961	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	4487026 Security	Critical	Remote Code Execution	4480961	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0651						
Version 1607 for x64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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-2019-0651						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4486996 Security Update	Critical	Remote Code Execution	4480978	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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-	4487017 Security Update	Critical	Remote Code Execution	4480966	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-2019-0651						
based Systems						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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-2019-0651						
Microsoft Edge on Windows Server 2019	4487044 Security Update	Moderate	Remote Code Execution	4480116	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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	Release Notes Security Update	Critical	Remote Code Execution	4480978	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-2019-0652 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0652 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 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. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0652						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0652						
Microsoft Edge on Windows 10 for 32-bit Systems	4487018 Security Update	Critical	Remote Code Execution	4480962	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	4487018 Security Update	Critical	Remote Code Execution	4480962	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	4487026 Security Update	Moderate	Remote Code Execution	4480961	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	4487026 Security Update	Critical	Remote Code Execution	4480961	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	4487026 Security	Critical	Remote Code Execution	4480961	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0652						
Version 1607 for x64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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-2019-0652						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4486996 Security Update	Critical	Remote Code Execution	4480978	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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-	4487017 Security Update	Critical	Remote Code Execution	4480966	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-2019-0652						
based Systems						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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-2019-0652						
Microsoft Edge on Windows Server 2019	4487044 Security Update	Moderate	Remote Code Execution	4480116	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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	Release Notes Security Update	Critical	Remote Code Execution	4480978	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-2019-0654 - Microsoft Browser Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0654 MITRE NVD	**CVE Title:** Microsoft Browser Spoofing Vulnerability **Description:** A spoofing vulnerability exists when Microsoft browsers improperly handles specific redirects. An attacker who successfully exploited this vulnerability could trick a user into believing that the user was on a legitimate website. The specially crafted website could either spoof content or serve as a pivot to chain an attack with other vulnerabilities in web services. To exploit the vulnerability, the user must either browse to a malicious website or be redirected to it. In an email attack scenario, an attacker could send an email message in an attempt to convince the user to click a link to a malicious site. In a web-based attack scenario, an attacker could host a specially crafted website designed to appear as a legitimate website to the user. However, the attacker would have no way to force the user to visit the specially crafted website. The attacker would have to convince the user to visit the specially crafted website, typically by way of enticement in an email or instant message. The security update addresses the vulnerability by correcting how browsers handles specific redirects.	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0654						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0654						
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	4486474 IE Cumulative 4487023 Monthly Rollup	Low	Spoofing	4480968	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4486474 IE Cumulative 4487023 Monthly Rollup	Low	Spoofing	4480968	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7	4486563 Monthly Rollup 4486474 IE	Important	Spoofing	4480965	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/RC:C	Yes

CVE-2019-0654						
for 32-bit Systems Service Pack 1	Cumulative					
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4486474 IE Cumulative 4486563 Monthly Rollup	Important	Spoofing	4480970	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/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4486474 IE Cumulative 4486563 Monthly Rollup	Low	Spoofing	4480970	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0654						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4486474 IE Cumulative 4487000 Monthly Rollup	Important	Spoofing	4480963	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/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4486474 IE Cumulative 4487000 Monthly Rollup	Important	Spoofing	4480963	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/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4486474 IE Cumulative 4487000 Monthly Rollup	Low	Spoofing	4480963	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4487000 Monthly Rollup	Important	Spoofing	4480963	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/RC:C	Yes

CVE-2019-0654						
Windows RT 8.1						
Internet Explorer 11 on Windows 10 for 32-bit Systems	4487018 Security Update	Important	Spoofing	4480962	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/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4487018 Security Update	Important	Spoofing	4480962	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/RC:C	Yes
Internet Explorer 11 on Windows Server 2016	4487026 Security Update	Low	Spoofing	4480961	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4487026 Security	Important	Spoofing	4480961	Base: 4.3 Temporal: 3.9	Yes

CVE-2019-0654						
Windows 10 Version 1607 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4487026 Security Update	Important	Spoofing	4480961	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/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Important	Spoofing	4480973	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/RC:C	Yes
Internet Explorer 11	4487020 Security	Important	Spoofing	4480973	Base: 4.3 Temporal: 3.9	Yes

CVE-2019-0654						
on Windows 10 Version 1703 for x64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4486996 Security Update	Important	Spoofing	4480978	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/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4486996 Security Update	Important	Spoofing	4480978	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/RC:C	Yes

CVE-2019-0654						
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Important	Spoofing	4480966	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/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4487017 Security Update	Important	Spoofing	4480966	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/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-	4487017 Security Update	Important	Spoofing	4480966	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/RC:C	Yes

CVE-2019-0654						
based Systems						
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Important	Spoofing	4480116	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/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Important	Spoofing	4480116	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/RC:C	Yes
Internet Explorer 11 on Windows 10 Version	4487044 Security Update	Important	Spoofing	4480116	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/RC:C	Yes

CVE-2019-0654						
1809 for ARM64-based Systems						
Internet Explorer 11 on Windows Server 2019	4487044 Security Update	Low	Spoofing	4480116	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems	4486996 Security Update	Important	Spoofing	4480978	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/RC:C	Yes
Internet Explorer 10 on Windows Server 2012	4486474 IE Cumulative 4487025 Monthly	Low	Spoofing	4480965	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0654						
	Rollup					
Microsoft Edge on Windows 10 for 32-bit Systems	4487018 Security Update	Important	Spoofing	4480962	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4487018 Security Update	Important	Spoofing	4480962	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2016	4487026 Security Update	Important	Spoofing	4480961	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for	4487026 Security Update	Important	Spoofing	4480961	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0654						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4487026 Security Update	Important	Spoofing	4480961	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Important	Spoofing	4480973	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4487020 Security Update	Important	Spoofing	4480973	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0654						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4486996 Security Update	Important	Spoofing	4480978	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4486996 Security Update	Important	Spoofing	4480978	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Important	Spoofing	4480966	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4487017 Security	Important	Spoofing	4480966	Base: 4.3 Temporal: 3.9	Yes

CVE-2019-0654						
Windows 10 Version 1803 for x64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4487017 Security Update	Important	Spoofing	4480966	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Important	Spoofing	4480116	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4487044 Security	Important	Spoofing	4480116	Base: 4.3 Temporal: 3.9	Yes

CVE-2019-0654						
10 Version 1809 for x64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4487044 Security Update	Important	Spoofing	4480116	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2019	4487044 Security Update	Important	Spoofing	4480116	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for ARM64-	4486996 Security Update	Important	Spoofing	4480978	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0654						
based Systems						

CVE-2019-0655 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0655 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 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	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0655						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4487018 Security Update	Critical	Remote Code Execution	4480962	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	4487018 Security Update	Critical	Remote Code Execution	4480962	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	4487026 Security Update	Moderate	Remote Code Execution	4480961	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	4487026 Security Update	Critical	Remote Code Execution	4480961	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-2019-0655						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4487026 Security Update	Critical	Remote Code Execution	4480961	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	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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-2019-0655						
for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4486996 Security Update	Critical	Remote Code Execution	4480978	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487017 Security	Critical	Remote Code Execution	4480966	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0655						
Version 1803 for ARM64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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-2019-0655						
Microsoft Edge on Windows Server 2019	4487044 Security Update	Moderate	Remote Code Execution	4480116	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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	Release Notes Security Update	Critical	Remote Code Execution	4480978	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-2019-0656 - Windows Kernel Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0656 MITRE NVD	**CVE Title:** Windows Kernel Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application to take control of an affected system. The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0656						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 8.1 for 32-bit systems	4487000 Monthly Rollup 4487028 Security Only	Important	Elevation of Privilege	4480963	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-2019-0656						
Windows 8.1 for x64-based systems	4487000 Monthly Rollup 4487028 Security Only	Important	Elevation of Privilege	4480963	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	4487000 Monthly Rollup 4487028 Security Only	Important	Elevation of Privilege	4480963	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	4487000 Monthly Rollup	Important	Elevation of Privilege	4480963	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)	4487000 Monthly Rollup 4487028 Security	Important	Elevation of Privilege	4480963	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-2019-0656						
	Only					
Windows 10 for 32-bit Systems	4487018 Security Update	Important	Elevation of Privilege	4480962	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	4487018 Security Update	Important	Elevation of Privilege	4480962	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	4487026 Security Update	Important	Elevation of Privilege	4480961	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	4487026 Security Update	Important	Elevation of Privilege	4480961	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	4487026 Security Update	Important	Elevation of Privilege	4480961	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-2019-0656						
Windows Server 2016 (Server Core installation)	4487026 Security Update	Important	Elevation of Privilege	4480961	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	4487020 Security Update	Important	Elevation of Privilege	4480973	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	4487020 Security Update	Important	Elevation of Privilege	4480973	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	4486996 Security Update	Important	Elevation of Privilege	4480978	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	4486996 Security Update	Important	Elevation of Privilege	4480978	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 1709	4486996 Security	Important	Elevation of Privilege	4480978	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0656						
(Server Core Installation)	Update				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	
Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Important	Elevation of Privilege	4480966	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	4487017 Security Update	Important	Elevation of Privilege	4480966	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)	4487017 Security Update	Important	Elevation of Privilege	4480966	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	4487017 Security Update	Important	Elevation of Privilege	4480966	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	4487044 Security	Important	Elevation of Privilege	4480116	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0656						
for 32-bit Systems	Update				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	
Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Important	Elevation of Privilege	4480116	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	4487044 Security Update	Important	Elevation of Privilege	4480116	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	4487044 Security Update	Important	Elevation of Privilege	4480116	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)	4487044 Security Update	Important	Elevation of Privilege	4480116	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-	4486996 Security	Important	Elevation of Privilege	4480978	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0656						
based Systems	Update				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	

CVE-2019-0657 - .NET Framework and Visual Studio Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0657 MITRE NVD	**CVE Title:** .NET Framework and Visual Studio Spoofing Vulnerability **Description:** A vulnerability exists in certain .Net Framework API's and Visual Studio in the way they parse URL's. An attacker who successfully exploited this vulnerability could use it to bypass security logic intended to ensure that a user-provided URL belonged to a specific hostname or a subdomain of that hostname. This could be used to cause privileged communication to be made to an untrusted service as if it was a trusted service. To exploit the vulnerability, an attacker must provide a URL string to an application that attempts to verify that the URL belongs to a specific hostname or to a subdomain of that hostname. The application must then make an HTTP request to the attacker-provided URL either directly or by sending a processed version of the attacker-provided URL to a web browser.	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0657						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0657						
Microsoft .NET Framework 4.5.2 on Windows 7 for 32-bit Systems Service Pack 1	4483455 Monthly Rollup 4483474 Security Only	Important	Spoofing	4481481; 4481488	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 7 for x64-based Systems Service Pack 1	4483455 Monthly Rollup 4483474 Security Only	Important	Spoofing	4481481; 4481488	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4483455 Monthly Rollup 4483474 Security Only	Important	Spoofing	4481481; 4481488	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4483455 Monthly Rollup 4483474	Important	Spoofing	4481481; 4481488	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0657						
	Security Only					
Microsoft .NET Framework 4.5.2 on Windows Server 2012	4483454 Monthly Rollup 4483473 Security Only	Important	Spoofing	4481483; 4481489	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation)	4483454 Monthly Rollup 4483473 Security Only	Important	Spoofing	4481483; 4481489	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems	4483472 Security Only 4483453 Monthly Rollup	Important	Spoofing	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems	4483472 Security Only 4483453	Important	Spoofing	4481485; 4481490	Base: N/A Temporal: N/A	Maybe

CVE-2019-0657						
	Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2	4483472 Security Only 4483453 Monthly Rollup	Important	Spoofing	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows RT 8.1	4483453 Monthly Rollup	Important	Spoofing	4481484; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation)	4483472 Security Only 4483453 Monthly Rollup	Important	Spoofing	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4483474 Security Only 4483455	Important	Spoofing	4481485; 4481490	Base: N/A Temporal: N/A	Maybe

CVE-2019-0657						
	Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for x64-based Systems Service Pack 2	4483474 Security Only 4483455 Monthly Rollup	Important	Spoofing	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2	4483470 Security Only 4483451 Monthly Rollup	Important	Spoofing	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6 on Windows Server 2008 for x64-based Systems Service Pack 2	4483470 Security Only 4483451 Monthly Rollup	Important	Spoofing	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
.NET Core 1.0	Release Notes Security	Important	Spoofing	4481485; 4481490	Base: N/A Temporal:	Maybe

CVE-2019-0657						
	Update				N/A Vector: N/A	
.NET Core 1.1	Release Notes Security Update	Important	Spoofing	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Visual Studio 2017	Release Notes Security Update	Important	Spoofing	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Important	Spoofing	4480966	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for x64-based Systems	4487017 Security Update	Important	Spoofing	4480966	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0657						
Microsoft .NET Framework 4.7.2 on Windows Server, version 1803 (Server Core Installation)	4487017 Security Update	Important	Spoofing	4480966	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for ARM64-based Systems	4487017 Security Update	Important	Spoofing	4480966	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1809 for 32-bit Systems	4483452 Monthly Rollup	Important	Spoofing	4480056; 4481031	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1809 for x64-based Systems	4483452 Monthly Rollup	Important	Spoofing	4480056; 4481031	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.2 on Windows Server 2019	4483452 Monthly	Important	Spoofing	4480056; 4481031	Base: N/A Temporal: N/A	Yes

CVE-2019-0657						
	Rollup				Vector: N/A	
Microsoft .NET Framework 4.7.2 on Windows Server 2019 (Server Core installation)	4483452 Monthly Rollup	Important	Spoofing	4480056; 4481031	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6/4.6.1/4.6.2 on Windows 10 for 32-bit Systems	4487018 Security Update	Important	Spoofing	4480962	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6/4.6.1/4.6.2 on Windows 10 for x64-based Systems	4487018 Security Update	Important	Spoofing	4480962	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for 32-bit Systems Service Pack 1	4483451 Monthly Rollup 4483470 Security Only	Important	Spoofing	4481481; 4481488	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0657						
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for x64-based Systems Service Pack 1	4483451 Monthly Rollup 4483470 Security Only	Important	Spoofing	4481481; 4481488	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4483451 Monthly Rollup 4483470 Security Only	Important	Spoofing	4481481; 4481488	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4483451 Monthly Rollup 4483470 Security Only	Important	Spoofing	4481481; 4481488	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012	4483449 Monthly Rollup 4483468	Important	Spoofing	4481483; 4481489	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0657						
	Security Only					
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 (Server Core installation)	4483449 Monthly Rollup 4483468 Security Only	Important	Spoofing	4481483; 4481489	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for 32-bit systems	4483469 Security Only 4483450 Monthly Rollup	Important	Spoofing	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for x64-based systems	4483469 Security Only 4483450 Monthly Rollup	Important	Spoofing	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2	4483469 Security Only 4483450	Important	Spoofing	4481485; 4481490	Base: N/A Temporal: N/A	Maybe

CVE-2019-0657						
	Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows RT 8.1	4483450 Monthly Rollup	Important	Spoofing	4481484; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2 (Server Core installation)	4483469 Security Only 4483450 Monthly Rollup	Important	Spoofing	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016	4487026 Security Update	Important	Spoofing	4480961	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for 32-bit Systems	4487026 Security Update	Important	Spoofing	4480961	Base: N/A Temporal: N/A	Yes

CVE-2019-0657						
					Vector: N/A	
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for x64-based Systems	4487026 Security Update	Important	Spoofing	4480961	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016 (Server Core installation)	4487026 Security Update	Important	Spoofing	4480961	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7/4.7.1/4.7.2 on Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Important	Spoofing	4480973	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7/4.7.1/4.7.2 on Windows 10 Version 1703 for x64-based Systems	4487020 Security Update	Important	Spoofing	4480973	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0657						
Microsoft .NET Framework 4.7.1/4.7.2 on Windows 10 Version 1709 for 32-bit Systems	4486996 Security Update	Important	Spoofing	4480978	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.1/4.7.2 on Windows 10 Version 1709 for x64-based Systems	4486996 Security Update	Important	Spoofing	4480978	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.1/4.7.2 on Windows Server, version 1709 (Server Core Installation)	4486996 Security Update	Important	Spoofing	4480978	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.1/4.7.2 on Windows 10 Version 1709 for ARM64-based Systems	4486996 Security Update	Important	Spoofing	4480978	Base: N/A Temporal: N/A Vector: N/A	Yes
.NET Core 2.1	Release Notes Security	Important	Spoofing	4480978	Base: N/A Temporal: N/A	Maybe

CVE-2019-0657						
	Update				Vector: N/A	
Microsoft Visual Studio 2017 version 15.9	Release Notes Security Update	Important	Spoofing	4480978	Base: N/A Temporal: N/A Vector: N/A	Maybe
.NET Core 2.2	Release Notes Security Update	Important	Spoofing	4480978	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012	4483456 Monthly Rollup 4483481 Security Only	Important	Spoofing	4481483; 4481489	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation)	4483456 Monthly Rollup 4483481	Important	Spoofing	4481483; 4481489	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0657						
	Security Only					
Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems	4483484 Security Only 4483459 Monthly Rollup	Important	Spoofing	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems	4483484 Security Only 4483459 Monthly Rollup	Important	Spoofing	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2	4483484 Security Only 4483459 Monthly Rollup	Important	Spoofing	4481485; 4481490	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation)	4483484 Security Only 4483459	Important	Spoofing	4481485; 4481490	Base: N/A Temporal: N/A	Maybe

CVE-2019-0657						
	Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows 10 for 32-bit Systems	4487018 Security Update	Important	Spoofing	4480962	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 for x64-based Systems	4487018 Security Update	Important	Spoofing	4480962	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server 2016	4487026 Security Update	Important	Spoofing	4480961	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for 32-bit Systems	4487026 Security Update	Important	Spoofing	4480961	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0657						
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for x64-based Systems	4487026 Security Update	Important	Spoofing	4480961	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Important	Spoofing	4480973	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for x64-based Systems	4487020 Security Update	Important	Spoofing	4480973	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for 32-bit Systems	4486996 Security Update	Important	Spoofing	4480978	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for x64-based Systems	4486996 Security	Important	Spoofing	4480978	Base: N/A Temporal: N/A	Yes

CVE-2019-0657						
	Update				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows Server, version 1709 (Server Core Installation)	4486996 Security Update	Important	Spoofing	4480978	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Important	Spoofing	4480966	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for x64-based Systems	4487017 Security Update	Important	Spoofing	4480966	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server, version 1803 (Server Core Installation)	4487017 Security Update	Important	Spoofing	4480966	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0657						
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for ARM64-based Systems	4487017 Security Update	Important	Spoofing	4480966	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1809 for 32-bit Systems	4483452 Monthly Rollup	Important	Spoofing	4480056; 4481031	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1809 for x64-based Systems	4483452 Monthly Rollup	Important	Spoofing	4480056; 4481031	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server 2019	4483452 Monthly Rollup	Important	Spoofing	4480056; 4481031	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server 2019 (Server Core installation)	4483452 Monthly	Important	Spoofing	4480056; 4481031	Base: N/A Temporal: N/A	Yes

CVE-2019-0657						
	Rollup				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for ARM64-based Systems	4486996 Security Update	Important	Spoofing	4480978	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2	4483482 Security Only 4483457 Monthly Rollup	Important	Spoofing	4467227; 4481487	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4483482 Security Only 4483457 Monthly Rollup	Important	Spoofing	4481487; 4481491	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2	4483482 Security Only 4483457 Monthly	Important	Spoofing	4481487; 4481491	Base: N/A Temporal: N/A	Maybe

CVE-2019-0657						
	Rollup				Vector: N/A	
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2	4483482 Security Only 4483457 Monthly Rollup	Important	Spoofing	4467227; 4481487	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows 7 for 32-bit Systems Service Pack 1	4483458 Monthly Rollup 4483483 Security Only	Important	Spoofing	4481481; 4481488	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows 7 for x64-based Systems Service Pack 1	4483458 Monthly Rollup 4483483 Security Only	Important	Spoofing	4481481; 4481488	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4483458 Monthly Rollup	Important	Spoofing	4481481; 4481488	Base: N/A Temporal: N/A	Maybe

CVE-2019-0657						
	4483483 Security Only				Vector: N/A	
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4483458 Monthly Rollup 4483483 Security Only	Important	Spoofing	4467224; 4481481	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4483458 Monthly Rollup 4483483 Security Only	Important	Spoofing	4481481; 4481488	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0658 - Scripting Engine Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0658 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:** **What type of information could be disclosed by this vulnerability?**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0658						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Important	Information Disclosure	4480973	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/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4487020 Security Update	Important	Information Disclosure	4480973	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/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4486996 Security Update	Important	Information Disclosure	4480978	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/RC:C	Yes
Microsoft Edge on	4486996 Security	Important	Information Disclosure	4480978	Base: 4.3 Temporal: 3.9	Yes

CVE-2019-0658						
Windows 10 Version 1709 for x64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Important	Information Disclosure	4480966	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/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4487017 Security Update	Important	Information Disclosure	4480966	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/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for	4487017 Security Update	Important	Information Disclosure	4480966	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/RC:C	Yes

CVE-2019-0658						
ARM64-based Systems						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Important	Information Disclosure	4480116	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/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Important	Information Disclosure	4480116	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/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-	4487044 Security Update	Important	Information Disclosure	4480116	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/RC:C	Yes

CVE-2019-0658						
based Systems						
Microsoft Edge on Windows Server 2019	4487044 Security Update	Low	Information Disclosure	4480116	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/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems	4486996 Security Update	Important	Information Disclosure	4480978	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/RC:C	Yes
ChakraCore	Release Notes Security Update	Important	Information Disclosure	4480978	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/RC:C	Maybe

CVE-2019-0659 - Windows Storage Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0659 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 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0659						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4487018 Security Update	Important	Elevation of Privilege	4480962	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4487018 Security	Important	Elevation of Privilege	4480962	Base: 7 Temporal: 6.3	Yes

CVE-2019-0659						
	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2016	4487026 Security Update	Important	Elevation of Privilege	4480961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4487026 Security Update	Important	Elevation of Privilege	4480961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4487026 Security Update	Important	Elevation of Privilege	4480961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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)	4487026 Security Update	Important	Elevation of Privilege	4480961	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4487020 Security Update	Important	Elevation of Privilege	4480973	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0659						
Windows 10 Version 1703 for x64-based Systems	4487020 Security Update	Important	Elevation of Privilege	4480973	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4486996 Security Update	Important	Elevation of Privilege	4480978	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4486996 Security Update	Important	Elevation of Privilege	4480978	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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 1709 (Server Core Installation)	4486996 Security Update	Important	Elevation of Privilege	4480978	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4487017 Security Update	Important	Elevation of Privilege	4480966	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0659						
Windows 10 Version 1803 for x64-based Systems	4487017 Security Update	Important	Elevation of Privilege	4480966	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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)	4487017 Security Update	Important	Elevation of Privilege	4480966	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4487017 Security Update	Important	Elevation of Privilege	4480966	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4487044 Security Update	Important	Elevation of Privilege	4480116	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4487044 Security Update	Important	Elevation of Privilege	4480116	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0659						
Windows 10 Version 1809 for ARM64-based Systems	4487044 Security Update	Important	Elevation of Privilege	4480116	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4487044 Security Update	Important	Elevation of Privilege	4480116	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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)	4487044 Security Update	Important	Elevation of Privilege	4480116	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4486996 Security Update	Important	Elevation of Privilege	4480978	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0660 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0660 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 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0660						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems	4486563 Monthly Rollup 4486564	Important	Information Disclosure	4480970	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-2019-0660						
Service Pack 1	Security Only					
Windows 7 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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)	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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-	4486563 Monthly Rollup 4486564	Important	Information Disclosure	4480970	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-2019-0660						
Based Systems Service Pack 1	Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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)	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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	4486993 Security Only 4487025	Important	Information Disclosure	4480968	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-2019-0660						
	Monthly Rollup					
Windows Server 2012 (Server Core installation)	4486993 Security Only 4487025 Monthly Rollup	Important	Information Disclosure	4480968	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	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487000 Monthly Rollup 4487028 Security	Important	Information Disclosure	4480963	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-2019-0660						
	Only					
Windows Server 2012 R2	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487000 Monthly Rollup	Important	Information Disclosure	4480963	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)	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487018 Security	Important	Information Disclosure	4480962	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0660						
	Update				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	
Windows 10 for x64-based Systems	4487018 Security Update	Important	Information Disclosure	4480962	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	4487026 Security Update	Important	Information Disclosure	4480961	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	4487026 Security Update	Important	Information Disclosure	4480961	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	4487026 Security Update	Important	Information Disclosure	4480961	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)	4487026 Security Update	Important	Information Disclosure	4480961	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-2019-0660						
Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Important	Information Disclosure	4480973	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	4487020 Security Update	Important	Information Disclosure	4480973	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	4486996 Security Update	Important	Information Disclosure	4480978	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	4486996 Security Update	Important	Information Disclosure	4480978	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 1709	4486996 Security Update	Important	Information Disclosure	4480978	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-2019-0660						
(Server Core Installation)						
Windows 10 Version 1803 for 32-bit Systems	4487017 Security Update	Important	Information Disclosure	4480966	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	4487017 Security Update	Important	Information Disclosure	4480966	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)	4487017 Security Update	Important	Information Disclosure	4480966	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	4487017 Security Update	Important	Information Disclosure	4480966	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-2019-0660						
Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Important	Information Disclosure	4480116	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	4487044 Security Update	Important	Information Disclosure	4480116	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	4487044 Security Update	Important	Information Disclosure	4480116	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	4487044 Security Update	Important	Information Disclosure	4480116	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)	4487044 Security Update	Important	Information Disclosure	4480116	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-2019-0660						
Windows 10 Version 1709 for ARM64-based Systems	4486996 Security Update	Important	Information Disclosure	4480978	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 Service Pack 2	4487023 Monthly Rollup 4487019 Security Only	Important	Information Disclosure	4480968	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	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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-	4487019 Security Only	Important	Information Disclosure	4480968	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0660						
based Systems Service Pack 2	4487023 Monthly Rollup				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	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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-2019-0661 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0661	**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 handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system. An authenticated attacker could exploit this vulnerability by running a specially crafted application. The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?** 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 02/12/2019 08:00:00		

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

Affected Software

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

CVE-2019-0661						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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	4486563 Monthly Rollup	Important	Information Disclosure	4480970	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0661						
Systems Service Pack 1	4486564 Security Only				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	
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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-2019-0661						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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)	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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	4486993 Security Only 4487025 Monthly Rollup	Important	Information Disclosure	4480968	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-2019-0661						
Windows Server 2012 (Server Core installation)	4486993 Security Only 4487025 Monthly Rollup	Important	Information Disclosure	4480968	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 Service Pack 2	4487023 Monthly Rollup 4487019 Security Only	Important	Information Disclosure	4480968	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	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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	4487019 Security	Important	Information Disclosure	4480968	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0661						
for x64-based Systems Service Pack 2	Only 4487023 Monthly Rollup				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	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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-2019-0662 - GDI+ Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0662 MITRE NVD	**CVE Title:** GDI+ Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory. An attacker who successfully exploited this vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. There are multiple ways an attacker could exploit the vulnerability: • In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability and then convince users to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to open an email attachment or click a link in an email or instant message.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	• In a file-sharing attack scenario, an attacker could provide a specially crafted document file that is designed to exploit the vulnerability, and then convince users to open the document file. The security update addresses the vulnerability by correcting the way that the Windows GDI handles objects in the memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0662						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Critical	Remote Code Execution	4480970	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 7 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Critical	Remote Code Execution	4480970	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-2019-0662						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4486563 Monthly Rollup 4486564 Security Only	Critical	Remote Code Execution	4480970	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	4486563 Monthly Rollup 4486564 Security Only	Critical	Remote Code Execution	4480970	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	4486563 Monthly Rollup 4486564 Security	Critical	Remote Code Execution	4480970	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-2019-0662						
Service Pack 1	Only					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4487019 Security Only 4487023 Monthly Rollup	Critical	Remote Code Execution	4480968	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	4486993 Security Only 4487025 Monthly Rollup	Critical	Remote Code Execution	4480968	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 (Server Core installation)	4486993 Security Only 4487025 Monthly	Critical	Remote Code Execution	4480968	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-2019-0662						
	Rollup					
Windows 8.1 for 32-bit systems	4487000 Monthly Rollup 4487028 Security Only	Critical	Remote Code Execution	4480963	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	4487000 Monthly Rollup 4487028 Security Only	Critical	Remote Code Execution	4480963	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	4487000 Monthly Rollup 4487028 Security Only	Critical	Remote Code Execution	4480963	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-2019-0662						
Windows RT 8.1	4487000 Monthly Rollup	Critical	Remote Code Execution	4480963	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)	4487000 Monthly Rollup 4487028 Security Only	Critical	Remote Code Execution	4480963	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	4487018 Security Update	Critical	Remote Code Execution	4480962	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	4487018 Security Update	Critical	Remote Code Execution	4480962	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	4487026 Security Update	Critical	Remote Code Execution	4480961	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-2019-0662						
Windows 10 Version 1607 for 32-bit Systems	4487026 Security Update	Critical	Remote Code Execution	4480961	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	4487026 Security Update	Critical	Remote Code Execution	4480961	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)	4487026 Security Update	Critical	Remote Code Execution	4480961	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	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4487020 Security Update	Critical	Remote Code Execution	4480973	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	4486996 Security	Critical	Remote Code Execution	4480978	Base: 8.8 Temporal: 7.9	Yes

CVE-2019-0662						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1709 for x64-based Systems	4486996 Security Update	Critical	Remote Code Execution	4480978	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 1709 (Server Core Installation)	4486996 Security Update	Critical	Remote Code Execution	4480978	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487017 Security Update	Critical	Remote Code Execution	4480966	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-2019-0662						
(Server Core Installation)						
Windows 10 Version 1803 for ARM64-based Systems	4487017 Security Update	Critical	Remote Code Execution	4480966	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4487044 Security	Critical	Remote Code Execution	4480116	Base: 8.8 Temporal: 7.9	Yes

CVE-2019-0662						
	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2019 (Server Core installation)	4487044 Security Update	Critical	Remote Code Execution	4480116	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	4486996 Security Update	Critical	Remote Code Execution	4480978	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 Itanium-Based Systems Service Pack 2	4487023 Monthly Rollup 4487019 Security Only	Critical	Remote Code Execution	4480968	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	4487019 Security Only 4487023 Monthly	Critical	Remote Code Execution	4480968	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-2019-0662						
Service Pack 2	Rollup					
Windows Server 2008 for x64-based Systems Service Pack 2	4487019 Security Only 4487023 Monthly Rollup	Critical	Remote Code Execution	4480968	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)	4487019 Security Only 4487023 Monthly Rollup	Critical	Remote Code Execution	4480968	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-2019-0664 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0664 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 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0664						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems	4486563 Monthly Rollup 4486564	Important	Information Disclosure	4480970	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-2019-0664						
Service Pack 1	Security Only					
Windows 7 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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)	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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	4486563 Monthly Rollup	Important	Information Disclosure	4480970	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0664						
Itanium-Based Systems Service Pack 1	4486564 Security Only				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	
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4486563 Monthly Rollup 4486564 Security Only	Important	Information Disclosure	4480970	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)	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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	4486993 Security	Important	Information Disclosure	4480968	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0664						
	Only 4487025 Monthly Rollup				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	
Windows Server 2012 (Server Core installation)	4486993 Security Only 4487025 Monthly Rollup	Important	Information Disclosure	4480968	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	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487000 Monthly Rollup 4487028	Important	Information Disclosure	4480963	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-2019-0664						
	Security Only					
Windows Server 2012 R2	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487000 Monthly Rollup	Important	Information Disclosure	4480963	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)	4487000 Monthly Rollup 4487028 Security Only	Important	Information Disclosure	4480963	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	4487023 Monthly	Important	Information Disclosure	4480968	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0664						
for Itanium-Based Systems Service Pack 2	Rollup 4487019 Security Only				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	
Windows Server 2008 for 32-bit Systems Service Pack 2	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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	4487019 Security Only 4487023 Monthly Rollup	Important	Information Disclosure	4480968	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	4487019 Security Only 4487023	Important	Information Disclosure	4480968	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-2019-0664						
Systems Service Pack 2 (Server Core installation)	Monthly Rollup					

CVE-2019-0668 - Microsoft SharePoint Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0668 MITRE NVD	**CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0668						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Enterprise Server 2016	4462155 Security Update	Important	Elevation of Privilege	4461598	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2013 Service Pack 1	4462139 Security Update	Important	Elevation of Privilege	4461591	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0669 - Microsoft Excel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0669 MITRE NVD	**CVE Title:** Microsoft Excel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory. An attacker who exploited the vulnerability could use the information to compromise the userâ€™s computer or data.	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, an attacker could craft a special document file and then convince the user to open it. An attacker must know the memory address location where the object was created. The update addresses the vulnerability by changing the way certain Excel functions handle objects in memory. **FAQ:** **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 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0669						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Excel 2010 Service Pack 2 (32-bit editions)	4462186 Security Update	Important	Security Feature Bypass	4461577	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2010 Service Pack 2 (64-bit editions)	4462186 Security Update	Important	Security Feature Bypass	4461577	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4462177 Security Update	Important	Security Feature Bypass	4461570	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4462177 Security Update	Important	Security Feature Bypass	4461570	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0669						
Microsoft Excel 2013 Service Pack 1 (32-bit editions)	4461597 Security Update	Important	Security Feature Bypass	4461559	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (64-bit editions)	4461597 Security Update	Important	Security Feature Bypass	4461559	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 RT Service Pack 1	4461597 Security Update	Important	Security Feature Bypass	4461559	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 for Mac	Release Notes Security Update	Important	Security Feature Bypass	4461559	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Excel 2016 (32-bit edition)	4462115 Security Update	Important	Security Feature Bypass	4461542	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 (64-bit edition)	4462115 Security Update	Important	Security Feature Bypass	4461542	Base: N/A Temporal:	Maybe

CVE-2019-0669						
					N/A Vector: N/A	
Microsoft Excel Viewer	4461608 Security Update	Important	Security Feature Bypass	4461566	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2019 for 32-bit editions	Click to Run Security Update	Important	Security Feature Bypass	4461566	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office 2019 for 64-bit editions	Click to Run Security Update	Important	Security Feature Bypass	4461566	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office 2019 for Mac	Release Notes Security Update	Important	Security Feature Bypass	4461566	Base: N/A Temporal: N/A Vector: N/A	No
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Security Feature Bypass	4461566	Base: N/A Temporal: N/A Vector: N/A	No

CVE-2019-0669						
Office 365 ProPlus for 64-bit Systems	Click to Run Security Update	Important	Security Feature Bypass	4461566	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office Compatibility Pack Service Pack 3	4461607 Security Update	Important	Security Feature Bypass	4461565	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0670 - Microsoft SharePoint Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0670 MITRE NVD	**CVE Title:** Microsoft SharePoint Spoofing Vulnerability **Description:** A spoofing vulnerability exists in Microsoft SharePoint when the application does not properly parse HTTP content. An attacker who successfully exploited this vulnerability could trick a user by redirecting the user to a specially crafted website. The specially crafted website could either spoof content or serve as a pivot the chain an attach with other vulnerabilities in web services.	Moderate	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, the user must click a specially crafted URL. In an application-based attack scenario, an attacker could manipulate specific parameters and create a specially crafted URL in attempt to convince the user to click it. In a web-based attack scenario, an attacker could host a specially crafted website designed to appear as a legitimate website to the user. However, the attacker would have no way to force the user to visit the specially crafted website. The attacker would have to convince the user to visit the specially crafted website, typically by way of enticement in an email or instant message, and then convince the user to interact with content on the website. The security update addresses the vulnerability by correcting how Microsoft SharePoint handles URL redirects. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00		

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

Affected Software

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

CVE-2019-0670						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Foundation 2013 Service Pack 1	4462143 Security Update	Moderate	Spoofing	4461596	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2013 Service Pack 1	4462139 Security Update	Moderate	Spoofing	4461591	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0671 - Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0671 MITRE NVD	**CVE Title:** Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Microsoft Office Access Connectivity 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 Microsoft Office Access Connectivity Engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0671						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4018313 Security Update	Important	Remote Code Execution	3114874	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4018313 Security Update	Important	Remote Code Execution	3114874	Base: N/A Temporal:	Maybe

CVE-2019-0671						
					N/A Vector: N/A	
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4018300 Security Update	Important	Remote Code Execution	3172459	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4018300 Security Update	Important	Remote Code Execution	3172459	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 RT Service Pack 1	4018300 Security Update	Important	Remote Code Execution	3172459	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (32-bit edition)	4018294 Security Update	Important	Remote Code Execution	4011143	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	4018294 Security Update	Important	Remote Code Execution	4011143	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0671						
Microsoft Office 2019 for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011143	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	4011143	Base: N/A Temporal: N/A Vector: N/A	No
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Remote Code Execution	4011143	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	4011143	Base: N/A Temporal: N/A Vector: N/A	No

CVE-2019-0672 - Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0672 MITRE NVD	**CVE Title:** Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Microsoft Office Access Connectivity 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 Microsoft Office Access Connectivity Engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0672						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4018313 Security Update	Important	Remote Code Execution	3114874	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4018313 Security Update	Important	Remote Code Execution	3114874	Base: N/A Temporal:	Maybe

CVE-2019-0672						
					N/A Vector: N/A	
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4018300 Security Update	Important	Remote Code Execution	3172459	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4018300 Security Update	Important	Remote Code Execution	3172459	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 RT Service Pack 1	4018300 Security Update	Important	Remote Code Execution	3172459	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (32-bit edition)	4018294 Security Update	Important	Remote Code Execution	4011143	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	4018294 Security Update	Important	Remote Code Execution	4011143	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0672						
Microsoft Office 2019 for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011143	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	4011143	Base: N/A Temporal: N/A Vector: N/A	No
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Remote Code Execution	4011143	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	4011143	Base: N/A Temporal: N/A Vector: N/A	No

CVE-2019-0673 - Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0673 MITRE NVD	**CVE Title:** Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Microsoft Office Access Connectivity 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 Microsoft Office Access Connectivity Engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0673						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4018313 Security Update	Important	Remote Code Execution	3114874	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4018313 Security Update	Important	Remote Code Execution	3114874	Base: N/A Temporal:	Maybe

CVE-2019-0673						
					N/A Vector: N/A	
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4018300 Security Update	Important	Remote Code Execution	3172459	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4018300 Security Update	Important	Remote Code Execution	3172459	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 RT Service Pack 1	4018300 Security Update	Important	Remote Code Execution	3172459	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (32-bit edition)	4018294 Security Update	Important	Remote Code Execution	4011143	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	4018294 Security Update	Important	Remote Code Execution	4011143	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0673						
Microsoft Office 2019 for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011143	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	4011143	Base: N/A Temporal: N/A Vector: N/A	No
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Remote Code Execution	4011143	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	4011143	Base: N/A Temporal: N/A Vector: N/A	No

CVE-2019-0674 - Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0674 MITRE NVD	**CVE Title:** Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Microsoft Office Access Connectivity 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 Microsoft Office Access Connectivity Engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0674						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4018313 Security Update	Important	Remote Code Execution	3114874	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4018313 Security Update	Important	Remote Code Execution	3114874	Base: N/A Temporal:	Maybe

CVE-2019-0674						
					N/A Vector: N/A	
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4018300 Security Update	Important	Remote Code Execution	3172459	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4018300 Security Update	Important	Remote Code Execution	3172459	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 RT Service Pack 1	4018300 Security Update	Important	Remote Code Execution	3172459	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (32-bit edition)	4018294 Security Update	Important	Remote Code Execution	4011143	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	4018294 Security Update	Important	Remote Code Execution	4011143	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0674						
Microsoft Office 2019 for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011143	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	4011143	Base: N/A Temporal: N/A Vector: N/A	No
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Remote Code Execution	4011143	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	4011143	Base: N/A Temporal: N/A Vector: N/A	No

CVE-2019-0675 - Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0675 MITRE NVD	**CVE Title:** Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Microsoft Office Access Connectivity 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 Microsoft Office Access Connectivity Engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0675						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4018313 Security Update	Important	Remote Code Execution	3114874	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4018313 Security Update	Important	Remote Code Execution	3114874	Base: N/A Temporal:	Maybe

CVE-2019-0675						
					N/A Vector: N/A	

CVE-2019-0676 - Internet Explorer Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0676 MITRE NVD	**CVE Title:** Internet Explorer Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory. An attacker who successfully exploited this vulnerability could test for the presence of files on disk. For an attack to be successful, an attacker must persuade a user to open a malicious website. The security update addresses the vulnerability by changing the way Internet Explorer handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The type of information that could be disclosed if an attacker successfully exploited this vulnerability is unauthorized file system access - reading from file system. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0676						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0676						
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4486563 Monthly Rollup 4486474 IE Cumulative	Important	Information Disclosure	4480965	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/RC:C	Yes
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4486474 IE Cumulative 4486563 Monthly Rollup	Important	Information Disclosure	4480970	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/RC:C	Yes
Internet Explorer 11 on Windows Server	4486474 IE Cumulative 4486563 Monthly	Low	Information Disclosure	4480970	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0676						
2008 R2 for x64-based Systems Service Pack 1	Rollup					
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4487000 Monthly Rollup 4486474 IE Cumulative	Important	Information Disclosure	4480965	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/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4486474 IE Cumulative 4487000 Monthly Rollup	Important	Information Disclosure	4480963	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/RC:C	Yes
Internet Explorer	4486474 IE Cumulative	Low	Information Disclosure	4480963	Base: 2.4 Temporal: 2.2	Yes

CVE-2019-0676						
11 on Windows Server 2012 R2	4487000 Monthly Rollup				Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows RT 8.1	4487000 Monthly Rollup	Important	Information Disclosure	4480963	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/RC:C	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4487018 Security Update	Important	Information Disclosure	4480962	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/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-	4487018 Security Update	Important	Information Disclosure	4480962	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/RC:C	Yes

CVE-2019-0676						
based Systems						
Internet Explorer 11 on Windows Server 2016	4487026 Security Update	Low	Information Disclosure	4480961	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4487026 Security Update	Important	Information Disclosure	4480961	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/RC:C	Yes
Internet Explorer 11 on Windows 10 Version	4487026 Security Update	Important	Information Disclosure	4480961	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/RC:C	Yes

CVE-2019-0676						
1607 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4487020 Security Update	Important	Information Disclosure	4480973	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/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4487020 Security Update	Important	Information Disclosure	4480973	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/RC:C	Yes

CVE-2019-0676						
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4486996 Security Update	Important	Information Disclosure	4480978	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/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4486996 Security Update	Important	Information Disclosure	4480978	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/RC:C	Yes
Internet Explorer 11 on Windows	4487017 Security Update	Important	Information Disclosure	4480966	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/RC:C	Yes

CVE-2019-0676						
10 Version 1803 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4487017 Security Update	Important	Information Disclosure	4480966	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/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-	4487017 Security Update	Important	Information Disclosure	4480966	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/RC:C	Yes

CVE-2019-0676						
based Systems						
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4487044 Security Update	Important	Information Disclosure	4480116	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/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4487044 Security Update	Important	Information Disclosure	4480116	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/RC:C	Yes
Internet Explorer	4487044 Security	Important	Information Disclosure	4480116	Base: 4.3 Temporal: 3.9	Yes

CVE-2019-0676						
11 on Windows 10 Version 1809 for ARM64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows Server 2019	4487044 Security Update	Low	Information Disclosure	4480116	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-	4486996 Security Update	Important	Information Disclosure	4480978	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/RC:C	Yes

CVE-2019-0676						
based Systems						
Internet Explorer 10 on Windows Server 2012	4486474 IE Cumulative 4487025 Monthly Rollup	Low	Information Disclosure	4480965	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0686 - Microsoft Exchange Server Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0686 MITRE NVD	**CVE Title:** Microsoft Exchange Server Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Microsoft Exchange Server. An attacker who successfully exploited this vulnerability could gain the same rights as any other user of the	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Exchange server. This could allow the attacker to perform activities such as accessing the mailboxes of other users. Exploitation of this vulnerability requires Exchange Web Services (EWS) and Push Notifications to be enabled and in use in an affected environment. To exploit the vulnerability, an attacker would need to execute a man-in-the-middle attack to forward an authentication request to a Microsoft Exchange Server, thereby allowing impersonation of another Exchange user. To address this vulnerability, Microsoft has changed the notifications contract established between EWS clients and Exchange Servers to not allow authenticated notifications to be streamed by the server. Instead, these notifications will be streamed using anonymous authentication mechanisms. **FAQ:** **Is this update related to Microsoft Security Advisory ADV190007?** The update associated with CVE-2019-0686 and CVE-2019-0724 resolve the vulnerability discussed in Microsoft Security Advisory ADV190007. Customers who have implemented the workaround listed in the Security Advisory are encouraged to remove it after applying this update to fully restore previous functionality. **Mitigations:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0686						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Exchange Server 2010 Service Pack 3 Update Rollup 26	4487052 Security Update	Important	Elevation of Privilege	4468742	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0686						
Microsoft Exchange Server 2013 Cumulative Update 22	4345836 Security Update	Important	Elevation of Privilege	4468742	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2016 Cumulative Update 12	4471392 Security Update	Important	Elevation of Privilege	4468742	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2019 Cumulative Update 1	4471391 Security Update	Important	Elevation of Privilege	4468742	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0724 - Microsoft Exchange Server Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0724 MITRE NVD	**CVE Title:** Microsoft Exchange Server Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Microsoft Exchange Server. An attacker who successfully exploited this vulnerability could gain the same rights as a Domain Administrator. Exploitation of this vulnerability requires Exchange Web Services (EWS) and Push Notifications to be enabled and in use in an affected environment. To exploit the vulnerability, an attacker would need to execute a man-in-the-middle attack to forward an authentication request to a Microsoft Active Directory domain controller, thereby facilitating gaining of increased privileges on the domain controller. To address this vulnerability, Microsoft has evaluated the rights granted to Exchange Servers and Exchange Administrators in the identified scenarios and determined changes are possible which lower the permissions granted within an Active Directory domain. The actual permission changes will vary based upon the version of Exchange Server in use. Please see https://support.microsoft.com/kb/4490059 for more information.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: **Is this update related to Microsoft Security Advisory ADV190007?** The update associated with CVE-2019-0686 and CVE-2019-0724 resolve the vulnerability discussed in Microsoft Security Advisory ADV190007. Customers who have implemented the workaround listed in the Security Advisory are encouraged to remove it after applying this update to fully restore previous functionality. **Mitigations:** **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0724						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Exchange Server 2010 Service Pack 3 Update Rollup 26	4487052 Security Update	Important	Elevation of Privilege	4468742	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2013 Cumulative Update 22	4345836 Security Update	Important	Elevation of Privilege	4468742	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2016 Cumulative Update 12	4471392 Security Update	Important	Elevation of Privilege	4468742	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2019 Cumulative Update 1	4471391 Security Update	Important	Elevation of Privilege	4468742	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0728 - Visual Studio Code Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0728 MITRE NVD	**CVE Title:** Visual Studio Code Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Visual Studio Code when it process environment variables after opening a project. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would need to convince a target to clone a repository and open it in Visual Studio Code. Attacker-specified code would execute when the target opened the integrated terminal. The update address the vulnerability by modifying the way Visual Studio Code handles environment variables. **FAQ:** None **Mitigations:** None	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0728						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Visual Studio Code	Release Notes Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0729 - Azure IoT Java SDK Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0729 MITRE NVD	**CVE Title:** Azure IoT Java SDK Elevation of Privilege Vulnerability **Description:** An Elevation of Privilege vulnerability exists in the way Azure IoT Java SDK generates symmetric keys for encryption, allowing an attacker to predict the randomness of the key. An attacker could derive the keys from the way they are generated and use them to access a user's IoT hub. This update addresses the vulnerability by randomizing the key generation within Azure IoT SDK. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00	Important	Elevation of Privilege

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

Affected Software

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

CVE-2019-0729						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Java SDK for Azure IoT	Release Notes Security Update	Important	Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0741 - Azure IoT Java SDK Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0741 MITRE NVD	**CVE Title:** Azure IoT Java SDK Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the way Azure IoT Java SDK logs sensitive information. An attacker can exploit this vulnerability if a user has exposed the logs on the internet (or an attacker was able to get the logs) and can use this information to compromise the device. This update addresses this vulnerability by not storing sensitive information in the logs. **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 device information like resource ids, sas tokens, user properties, and other sensitive information. **Mitigations:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0741						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Java SDK for Azure IoT	Release Notes Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0742 - Team Foundation Server Cross-site Scripting Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0742 MITRE NVD	**CVE Title:** Team Foundation Server Cross-site Scripting Vulnerability **Description:** A Cross-site Scripting (XSS) vulnerability exists when Team Foundation Server does not properly sanitize user provided input. An authenticated attacker could exploit the vulnerability by sending a specially crafted payload to the Team Foundation Server, which will get executed in the context of the user every time a user visits the compromised page. 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, execute malicious code, and use the victim's identity to take actions on the site on behalf of the user, such as change permissions and delete content. The security update addresses the vulnerability by ensuring that Team Foundation Server sanitizes user inputs. **FAQ:** None **Mitigations:**	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0742						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Team Foundation Server 2018 Update 3.2	Release Notes Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0743 - Team Foundation Server Cross-site Scripting Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0743 MITRE NVD	**CVE Title:** Team Foundation Server Cross-site Scripting Vulnerability **Description:** A Cross-site Scripting (XSS) vulnerability exists when Team Foundation Server does not properly sanitize user provided input. An authenticated attacker could exploit the vulnerability by sending a specially crafted payload to the Team Foundation Server, which will get executed in the context of the user every time a user visits the compromised page. 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, execute malicious code, and use the victim's identity to take actions on the site on behalf of the user, such as change permissions and delete content. The security update addresses the vulnerability by ensuring that Team Foundation Server sanitizes user inputs. **FAQ:** None **Mitigations:**	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 02/12/2019 08:00:00 Information published.		

Affected Software

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

CVE-2019-0743						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Team Foundation Server 2018 Update 3.2	Release Notes Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe

Statement

==========

This advisory is only used to describe a potential risk. NSFOCUS does not provide any commitment or promise on this advisory. NSFOCUS and the author will not bear any liability for any direct and/or indirect consequences and losses caused by transmitting and/or using this advisory. NSFOCUS reserves all the rights to modify and interpret this advisory. Please include this statement paragraph when reproducing or transferring this advisory. Do not modify this advisory, add/delete any information to/from it, or use this advisory for commercial purposes without permission from NSFOCUS.

About NSFOCUS

==========

NSFOCUS IB is a wholly owned subsidiary of NSFOCUS, an enterprise application and network security provider, with operations in the Americas, Europe, the Middle East, Southeast Asia and Japan. NSFOCUS IB has a proven track record of combatting the increasingly complex cyber threat landscape through the construction and implementation of multi-layered defense systems. The company's Intelligent Hybrid Security strategy utilizes both cloud and on-premises security platforms, built on a foundation of real-time global threat intelligence, to provide unified, multi-layer protection from advanced cyber threats.

For more information about NSFOCUS, please visit:

QR code of NSFOCUS at Sina Weibo

QR code of NSFOCUS at WeChat