微软发布 10 月补丁修复 66 个安全问题

安全威胁通告

发布时间：2017 年 10 月 11 日

综述

微软于周二发布了 10 月安全更新补丁，修复了 66 个 Windows 的安全问题，产品涉及 Device Guard、Internet Explorer、Microsoft Edge、Microsoft Graphics Component、Microsoft JET Database Engine、Microsoft Office、Microsoft Scripting Engine、Microsoft Windows DNS、Microsoft Windows Search Component、Windows NTLM、Windows Shell、Windows SMB Server、Windows Subsystem for Linux 以及 Windows TPM。

相关信息如下（红色部分威胁相对比较高）：

产品	CVE 编号	CVE 标题
Device Guard	CVE-2017-11823	Microsoft Windows 安全功能绕过漏洞
Device Guard	CVE-2017-8715	Windows 安全功能绕过漏洞
Internet Explorer	CVE-2017-11822	Internet Explorer 内存破坏漏洞
Internet Explorer	CVE-2017-11790	Internet Explorer 信息泄露漏洞
Internet Explorer	CVE-2017-11810	Scripting Engine 内存破坏漏洞
Internet Explorer	CVE-2017-11813	Internet Explorer 内存破坏漏洞
Microsoft Edge	CVE-2017-8726	Microsoft Edge 内存破坏漏洞

Microsoft Edge	CVE-2017-11794	Microsoft Edge 信息泄露漏洞
Microsoft Graphics Component	CVE-2017-8693	Microsoft Graphics 信息泄露漏洞
Microsoft Graphics Component	CVE-2017-11762	Microsoft Graphics 远程代码执行漏洞
Microsoft Graphics Component	CVE-2017-11763	Microsoft Graphics 远程代码执行漏洞
Microsoft Graphics Component	CVE-2017-11816	Windows GDI 信息泄露漏洞
Microsoft Graphics Component	CVE-2017-11824	Windows Graphics Component 特权提升漏洞
Microsoft JET Database Engine	CVE-2017-8717	Microsoft JET Database Engine 远程代码执行漏洞

Microsoft JET Database Engine	CVE-2017-8718	Microsoft JET Database Engine 远程代码执行漏洞
Microsoft Office	ADV170017	Office Defense 深度更新
Microsoft Office	CVE-2017-11786	Skype for Business 特权提升漏洞
Microsoft Office	CVE-2017-11774	Microsoft Outlook 安全功能绕过漏洞
Microsoft Office	CVE-2017-11775	Microsoft Office SharePoint XSS 漏洞
Microsoft Office	CVE-2017-11776	Microsoft Outlook 信息泄露漏洞
Microsoft Office	CVE-2017-11777	Microsoft Office SharePoint XSS 漏洞

Microsoft Office	CVE-2017-11820	Microsoft Office SharePoint XSS 漏洞
Microsoft Office	CVE-2017-11825	Microsoft Office 远程代码执行漏洞
Microsoft Office	CVE-2017-11826	Microsoft Office 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11821	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11792	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11793	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11796	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11797	Scripting Engine 信息泄露漏洞

Microsoft Scripting Engine	CVE-2017-11798	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11799	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11800	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11801	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11802	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11804	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11805	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11806	Scripting Engine 内存破坏漏洞

Microsoft Scripting Engine	CVE-2017-11807	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11808	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11809	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11811	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11812	Scripting Engine 内存破坏漏洞
Microsoft Windows	ADV170016	Windows Server 2008 Defense 深度更新
Microsoft Windows	CVE-2017-11769	TRIE 远程代码执行漏洞
Microsoft Windows	CVE-2017-11783	Windows 特权提升漏洞

Microsoft Windows	CVE-2017-11818	Windows Storage 安全功能绕过漏洞
Microsoft Windows DNS	CVE-2017-11779	Windows DNSAPI 远程代码执行漏洞
Microsoft Windows Search Component	CVE-2017-11771	Windows Search 远程代码执行漏洞
Microsoft Windows Search Component	CVE-2017-11772	Microsoft Search 信息泄露漏洞
Windows Kernel	CVE-2017-11765	Windows Kernel 信息泄露漏洞
Windows Kernel	CVE-2017-11784	Windows Kernel 信息泄露漏洞
Windows Kernel	CVE-2017-11785	Windows Kernel 信息泄露漏洞
Windows Kernel	CVE-2017-11814	Windows Kernel 信息泄露漏洞

Windows Kernel	CVE-2017-11817	Windows 信息泄露漏洞
Windows Kernel-Mode Drivers	CVE-2017-8689	Win32k 特权提升漏洞
Windows Kernel-Mode Drivers	CVE-2017-8694	Win32k 特权提升漏洞
Windows NTLM	ADV170014	Optional Windows NTLM SSO 授权改变漏洞
Windows Shell	CVE-2017-8727	Windows Shell 内存破坏漏洞
Windows Shell	CVE-2017-11819	Windows Shell 远程代码执行漏洞
Windows SMB Server	CVE-2017-11780	Windows SMB 远程代码执行漏洞
Windows SMB Server	CVE-2017-11781	Windows SMB 拒绝服务漏洞

Windows SMB Server	CVE-2017-11782	Windows SMB 特权提升漏洞
Windows SMB Server	CVE-2017-11815	Windows SMB 信息泄露漏洞
Windows Subsystem for Linux	CVE-2017-8703	Windows Subsystem for Linux 拒绝服务漏洞
Windows TPM	ADV170012	TPM 安全功能绕过漏洞
Windows Update	CVE-2017-11829	Windows Update Delivery Optimization 特权提升漏洞

修复建议

微软官方已经发布更新补丁，请及时进行补丁更新。

附件

ADV170012 - Vulnerability in TPM could allow Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV170012 MITRE NVD	**CVE Title:** Vulnerability in TPM could allow Security Feature Bypass **Description:**	Critical	Security Feature Bypass

Executive Summary

A security vulnerability exists in certain Trusted Platform Module (TPM) chipsets.Â The vulnerability weakens key strength. It is important to note that this is a firmware vulnerability, and not a vulnerability in the operating system or a specific application. After you have installed software and/or firmware updates, you will need to re-enroll in any security services you are running to remediate those services. For more details contact the TPM manufacturer - https://www.infineon.com/TPM-update. For specific services and use cases that are rendered insecure, see "Step 5 - Remediate services/(Use cases)" under **Recommended Actions**.

Advisory Details

Important This vulnerability is present in a specific vendorâ€™sÂ TPM firmware that is based on Trusted Computing Guidelines (TCG) specification family 1.2 and 2.0, not in the TPM standard or in Microsoft Windows. Some Windows security features and potentially third-party software rely on keys generated by the TPM (if available on the system). Microsoft is releasing Windows security updates to help work around the vulnerability by logging events and by allowing the generation of software based keys. Even after the operating system and/or TPM firmware updates are installed, you will need to carry out additional remediation steps to force regeneration of previously created weak TPM keys,

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	depending on the applicable services you are running and on your particular use-cases. See Step 5 - "Remediate services based on your particular use cases" under **Recommended Actions**. FAQ **1. What systems are at risk from this vulnerability?** • **Client Operating Systems Windows** client systems are at increased risk due to the prevalence of TPM on client hardware systems. There are distinct advantages to using hardware encryption modules. • **Server Operating Systems** Servers with TPM modules. **2. What is a TPM?** See Trusted Platform Module Technology Overview **3. What is the associated CVE for this vulnerability?** See https://www.infineon.com/TPM-update **4. Have there been any active attacks detected?**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	No. When this security advisory was issued, Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers. **5. Has this vulnerability been publicly disclosed?** No. Microsoft received information about the vulnerability through coordinated vulnerability disclosure. **6. What is the CVSS score?** https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC:H/MPR:N/MUI:N/MS:U/MC:H/MI:L/MA:L **7. What if a TPM firmware update is not available from my hardware OEM?** Hardware OEMs may release a TPM firmware update independently of the Microsoft software updates. The software updates are being released as a workaround to the vulnerability. To address the underlying issue, customers need to obtain and install a TPM firmware update. It is recommended that you contact your hardware manufacturer(s) for further guidance. TPM firmware updates may be combined with OEM system firmware updates or be delivered as a standalone tool by OEMs. In the event of a hardware OEM explicitly NOT issuing a firmware update, customers can: • Decide that the operating system update (that generates software-based keys) is sufficient for your services and use-cases. **Note** Services and use-case remediation will still be necessary.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	• Move critical roles and users to devices that have updated firmware • Move critical roles and users to devices that are not impacted by this vulnerability **8. I am running Windows 7 or Windows Server 2007 R2. Why do these operating systems not appear on the Affected Products table?** Windows 7 services and use cases are limited to BitLocker. Bitlocker on Windows 7 cannot work around the hardware issue. Therefore, because the vulnerability is in the firmware, updates are only necessary for the firmware. For customers with affected devices that are running Windows 7, Microsoft suggests the following actions: • Move critical roles and users to devices that have updated firmware • Move critical roles and users to devices that are not affected by this vulnerability If you are using non-Microsoft apps that require a TPM, you should contact the app developer to see if the app is affected. **9. I am running Windows Server 2012, Windows Server 2012 R2, or Windows 8.1. Why are there two Security Updates listed in the Affected Products table for these operating systems?** The updates addressing this vulnerability are part of an industry-wide coordinated disclosure to remediate the vulnerability. Each Security Update addresses a different aspect of the vulnerability, and		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	were released in a phased approach. **Important:** Because the Security Updates are not cumulative, customers who install these updates must install both September and October updates to receive all of the updates for this vulnerability. **10. What do each of the Security Updates for Windows Server 2012, Windows Server 2012 R2, and Windows 8.1 address?** • September 2017 Security Updates provide the functionality to generate software keys. • October 2017 Security Updates provide detection in TPM.MSC to determine if your device has a vulnerable TPM module. It is recommended that you install **BOTH** Security Updates. Note that the Monthly Updates are cumulative, while Security Updates are not. Customers who install the monthly updates will receive both updates for this vulnerability. ## Recommended Actions **1. Apply the Windows operating system updates (see Affected Products table for specific package KB numbers) first**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

	WARNING: Do **NOT** apply the TPM firmware update prior to applying the Windows operating system mitigation update. Doing so will render your system unable to determine if your system is affected. You will need this information to conduct full remedation.
	
	• The mitigation and detection update for Windows:
	  ○ Addresses the vulnerability by preventing the generation of weak keys by the TPM hardware. New keys are generated using a software algorithm. Microsoft recommends that customers running systems that use affected TPM chipsets install the Windows security update as an interim measure until a firmware update is available from the system manufacturer.
	  ○ Generates event log entries when a vulnerable TPM is detected.
	  ○ Does NOT reduce BitLocker risk.
	
	The majority of customers have automatic updating enabled and will not need to take any action because the updates will be downloaded and installed automatically. Customers who have not enabled automatic updating need to check for updates and install applicable updates manually. For administrators and enterprise installations, or end users who want to install the updates manually, Microsoft recommends applying the update immediately using update management software, or by checking for updates using the Microsoft Update service. For more information on how to manually apply this specific update, see the Affected Products table.
	
	2. Determine devices in your organization that are affected		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Because both mobile and stationary systems may be affected, mixing reactive and proactive measures may be best to determine affected devices. Depending on your use-case scenario, Microsoft recommends that you use one of the following methods to determine affected devices. a. Option 1 - Use event log entries. After the applicable Windows update is applied, the system will generate Event ID 1794 in the Event Viewer after each reboot under **Windows Logs - System** when vulnerable firmware is identified. **Type** **Value** Event Log Windows Log/System Event Source TPM-WMI Event ID 1794 **NOTE**: Microsoft recommends that enterprise or home office users leverage this step as a reactive method to identify affected software. b. Option 2 - Use a script (See **Additional Context**) to detect if firmware on your systems contain the vulnerability. **NOTE**: Microsoft recommends that enterprise users leverage this step as a proactive method to identify affected software.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	c. Option 3 - Manually check the Trusted Platform Module (TPM) Management snap-in (TPM.MSC) on each Windows 10 device OOn devices running Windows 10 that have the October 2017 security update installed, in a CMD prompt, type "TPM.MSC" to open the Trusted Platform Module (TPM) Management snap-in. Devices with affected TPM modules will display the following error message: "The TPM is ready for use. The TPM firmware on this PC has a known security problem. Please contact your PC manufacturer to find out if an update is available. For more information please go to https://go.microsoft.com/fwlink/?linkid=852572." **NOTE**: Microsoft recommends that consumers and Home office users leverage this step to identify affected software. **3. If you determine that devices in your organization are affected, analyze your risk tolerance and create short and long term resolution plans** A firmware update may or may not be available at the time of advisory release. Furthermore, the affected devices may represent a only small portion of your overall resources. Even though the Windows update is not a true replacement for fixing the firmware flaw it can be used as a temporary mitigation. However, even after the operating system and TPM firmware updates are installed, you will need to assess your TPM usage scenarios and take manual actions to force new keys to be generated **4. Apply applicable firmware updates**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	• If your hardware is a Surface device, firmware updates are yet not available as of October 10, 2017. Microsoft is working to make firmware updates available for affected devices and will provide links in this advisory when the updates become available. Note that the Surface Laptop and the Surface Pro (released in June 2017) are NOT affected by this vulnerability. • If your device is not from Microsoft, apply the firmware provided by the OEM. • If your device OEM is not listed in the following table, please contact the OEM's Customer Support. **OEM** — **Link for firmware update** TPM OEM — https://www.infineon.com/TPM-update Fujitsu — http://www.fujitsu.com/global/support/products/software/security/products-f/ifsa-201701e.html HP — https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fsupport.hp.com%2Fus-en%2Fdocument%2Fc05792935&data=02%7C01%7Cagalva%40microsoft.com%7C8c5feb8668fc8d50fe6d602%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C636432406470417651&sdata=vrl9AF9sstnfvP5vzu66aD63g9PXpCZ8uY%2F55Zw%3D&reserved=0 **5. Remediate services based on your particular use cases** Microsoft will continue to provide additional support to help identify and remediate this issue as it becomes available. The following		

<table>
<tr><th>CVE ID</th><th>Vulnerability Description</th><th>Maximum Severity Rating</th><th>Vulnerability Impact</th></tr>
<tr><td></td><td>table contains a list of services that you may be running on your device and a link to instructions for applying remediation steps for that service.

IMPORTANT BEFORE any remedition steps can be taken, Microsoft strongly recommends that a firmware update be applied. This is not a simple one-step procedure and you should fully understand the scope of the impact to you before proceeding.

<table><tr><th>SERVICE</th><th>REMEDIATION STEPS</th></tr><tr><td>Active Directory Certificate Services (ADCS)</td><td>https://support.microsoft.com/en-us/help/4047409</td></tr><tr><td>Active Directory Directory Services (ADDS)</td><td>https://support.microsoft.com/en-us/help/4046462</td></tr><tr><td>BitLocker</td><td>https://support.microsoft.com/en-us/help/4046783</td></tr><tr><td>Credential Guard/DPAPI/Windows Information Protection</td><td>https://docs.microsoft.com/en-us/windows/access-protection/credenti guard/credential-guard-considerations#clearing-tpm-considerations</td></tr><tr><td>Device Health Attestation Service (DHA)</td><td>This vulnerability may impact the validity of the DHA-report that is issu Device Health Attestation Service. The DHA-report cannot be trusted w originating device is Jailbroken and DHA-Service is configured to perfc attestation in â€œAIKCert validation modeâ€. To address the issue pl DHA-Cloud or configure your organization's On Premise DHA-Service</td></tr></table></td><td></td><td></td></tr>
</table>

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	â€œ EKCert validationâ€ mode, and update your TPM firmware to address the root cause of the vulnerability. VSC - Virtual Smart Card https://support.microsoft.com/en-us/help/4046784 Windows Hello For Business and Azure Active Directory Â https://support.microsoft.com/en-us/help/4046168 Windows Hello (and Microsoft Accounts (MSA)) Documentation under review. Microsoft will update the advisory when it becomes available. Windows Server 2016 Domain-joined device public key authentication Domain-joined Device Public Key Authentication **6. Clear TPM** **Important**: Before using one of these methods for clearing TPM, please take note of the following: • Be aware that clearing a TPM will render ALL services that use TPM keys unusable until you complete any required remeditation steps. You may need to contact any third-party service vendors for those steps. • For systems running Windows 7, you must suspend BitLocker protection before clearing TPM from the operating system. See Suspend-BitLocker • For systems running Windows Server 2012, Windows Server 2012 R2, or Windows 8.1, it is not necessary to suspend BitLocker before clearing TPM from the operating system. It is not		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	recommended that you clear the TPM from a firmware menu because if you have activated Device Encryption, you will be unable to suspend it in the operating system. Additionally, you will need to retrieve your Device Encryption Recovery Key from the MSA cloud to boot after clearing the TPM. • Devices running Windows 10 that are protected by Credential Guard will lose secrets. For more information, see Credential Guard Considerations: Clearing TPM considerations. • To clear TPM via powershell, see Clear-Tpm • To clear TPM via GUI, see Clear all the keys from the TPM ## Additional context • Azure AD - What is Azure Active Directory? • Bitlocker suspension - Suspend-BitLocker • Credential Guard: Clearing TPM considerations - Clearing TPM Considerations • Domain-joined Device Public Key Authentication - Automatic public key provisioning • MSA Microsoft Account- Microsoft Accounts • TPM - Windows Trusted Platform Module Management Step-by-Step Guide • TPM Key Attestation - TPM Key Attestation • Virtual Smart Card overview - Virtual Smart Card Overview		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

	• Windows hello / Next Gen Credential - Windows Hello for Business
	
	Quick methods for determining the firmware version:
	
	• Use PowerShell cmd: Get-TPM (run as an administrator) on each device.
	• Use the following PowerShell script, run as an administrator. Failing to run the script as an administrator will return a false positive.
	
	`$IfxManufacturerIdInt = 0x49465800 # 'IFX'`
	
	`function IsInfineonFirmwareVersionAffectedRiemann ($FirmwareVersion)`
	`{`
	`$FirmwareMajor = $FirmwareVersion[0]`
	`$FirmwareMinor = $FirmwareVersion[1]`
	`switch ($FirmwareMajor)`
	`{`
	`4 { return $FirmwareMinor -le 33 -or ($FirmwareMinor -ge 40 -and $FirmwareMinor -le 42) }`
	`5 { return $FirmwareMinor -le 61 }`
	`6 { return $FirmwareMinor -le 42 }`
	`7 { return $FirmwareMinor -le 61 }`
	`133 { return $FirmwareMinor -le 32 }`		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

```
                        default { return $False }
                }
        }

        function IsInfineonFirmwareVersionRiemannSusceptible ($FirmwareMajor)
        {
                switch ($FirmwareMajor)
                {
                        4 { return $True }
                        5 { return $True }
                        6 { return $True }
                        7 { return $True }
                        133 { return $True }
                        default { return $False }
                }
        }

        $Tpm = Get-Tpm
        $ManufacturerIdInt = $Tpm.ManufacturerId
        $FirmwareVersion = $Tpm.ManufacturerVersion -split "\."
```

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

	$FirmwareVersionAtLastProvision = (Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\TPM\WMI" -Name "FirmwareVersionAtLastProvision" -ErrorAction SilentlyContinue).FirmwareVersionAtLastProvision
	
	if (!$Tpm)
	{
	Write-Host "No TPM found on this system, so the Riemann issue does not apply here."
	}
	else
	{
	if ($ManufacturerIdInt -ne $IfxManufacturerIdInt)
	{
	Write-Host "This non-Infineon TPM is not affected by the Riemann issue."
	}
	else
	{
	if ($FirmwareVersion.Length -lt 2)
	{		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

	Write-Error "Could not get TPM firmware version from this TPM."
	}
	else
	{
	if (IsInfineonFirmwareVersionRiemannSusceptible($FirmwareVersion[0]))
	{
	if (IsInfineonFirmwareVersionAffectedRiemann($FirmwareVersion))
	{
	Write-Host ("This Infineon firmware version {0}.{1} TPM is not safe. Please update your firmware." -f [int]$FirmwareVersion[0], [int]$FirmwareVersion[1])
	}
	else
	{
	Write-Host ("This Infineon firmware version {0}.{1} TPM is safe." -f [int]$FirmwareVersion[0], [int]$FirmwareVersion[1])
	if (!$FirmwareVersionAtLastProvision)
	{		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

	Write-Host ("We cannot determine what the firmware version was when the TPM was last cleared. Please clear your TPM now that the firmware is safe.")
	}
	elseif ($FirmwareVersion -ne $FirmwareVersionAtLastProvision)
	{
	Write-Host ("The firmware version when the TPM was last cleared was different from the current firmware version. Please clear your TPM now that the firmware is safe.")
	}
	}
	}
	else
	{
	Write-Host ("This Infineon firmware version {0}.{1} TPM is safe." -f [int]$FirmwareVersion[0], [int]$FirmwareVersion[1])
	}
	}
	}
	}		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

ADV170012						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012	4038786 Security Only 4041679 Security	Critical	Security Feature Bypass	4038799	Base: N/A Temporal:	Yes

ADV170012						
	Only 4041690 Monthly Rollup				N/A Vector: N/A	
Windows 8.1 for 32-bit systems	4038793 Security Only 4041687 Security Only 4041693 Monthly Rollup	Critical	Security Feature Bypass	4038792	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 8.1 for x64-based systems	4038793 Security Only 4041687 Security Only 4041693 Monthly Rollup	Critical	Security Feature Bypass	4038792	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 R2	4038793 Security Only 4041687 Security Only 4041693 Monthly	Critical	Security Feature Bypass	4038792	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV170012						
	Rollup					
Windows RT 8.1	4041693 Monthly Rollup	Critical	Security Feature Bypass	4038792	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 for 32-bit Systems	4042895 Security Update	Critical	Security Feature Bypass	4038781	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 for x64-based Systems	4042895 Security Update	Critical	Security Feature Bypass	4038781	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1511 for x64-based Systems	4041689 Security Update	Critical	Security Feature Bypass	4038783	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1511 for 32-bit Systems	4041689 Security Update	Critical	Security Feature Bypass	4038783	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV170012						
Windows Server 2016	4041691 Security Update	Critical	Security Feature Bypass	4038782	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1607 for 32-bit Systems	4041691 Security Update	Critical	Security Feature Bypass	4038782	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1607 for x64-based Systems	4041691 Security Update	Critical	Security Feature Bypass	4038782	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1703 for 32-bit Systems	4041676 Security Update	Critical	Security Feature Bypass	4038788	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1703 for x64-based Systems	4041676 Security Update	Critical	Security Feature Bypass	4038788	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV170014 - Optional Windows NTLM SSO authentication changes

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV170014 MITRE NVD	**CVE Title:** Optional Windows NTLM SSO authentication changes **Description:** Microsoft is releasing an optional security enhancement to NT LAN Manager (NTLM), limiting which network resources various clients in the Windows 10 or the Windows Server 2016 operating systems can use NTLM Single Sign On(SSO) as an authentication method. When you deploy the new security enhancement with a Network Isolation Policy defining your organization's resources, attackers can no longer redirect a user to a malicious resource outside your organization to obtain the NTLM authentication messages. This new behavior is optional, and requires customers who wish to enable it to opt in via a Windows Registry Setting or other means described below. Customers should be aware that enabling this new behavior will prevent NTLM SSO authentication with resources that are not marked as internal by the Windows Firewall. This may break some functionality by preventing NTLM SSO authentication to resources marked external, though other authentication methods will remain available. Examples where NTLM SSO authentication appear would be Internet Explorer or Edge, or a service calling WinHTTP to access a web resource; a user trying to connect to an SMB file share; or processes making RPC calls. Microsoft is releasing this new functionality as a mitigation to NTLM dictionary attacks. Microsoft continues to recommend that customers	Unknown	Unknown

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	move to public key authentication methods for applications which do not support modern authentication, and use negotiate with Kerberos authentication whenever possible. The new functionality works by denying NTLM SSO authentication as a method for public resources. This is achieved when the NTLM client leverages the Windows Firewallâ€™s ability to determine if a resource is a Public, Private, or Enterprise resource as defined by the customer-configured Windows Information Protection settings. Depending on this determination, the connection will either be allowed or denied. FAQ **1. Which registry setting should I set to enable this behavior?** Customers can add a DWORD32 key named â€œEnterpriseAccountSSOâ€ to the Windows Registry location HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0 with the following options: • 2 -Always allow SSO. (This is the default state.)		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	• 1 -Deny SSO if the resource is public. Allow if the resource is private or enterprise. **Allow** SSO if the resource is unspecified. • 0 - Deny SSO if the resource is public. Allow if the resource is private or enterprise. **Deny** SSO if the resource is unspecified. **2. Is any other configuration necessary for this new behavior?** Yes. Customers need to configure a Network Isolation Policy(NIP) that defines which networks should be considered internal/enterprise and thus will permit NTLM as an SSO Authentication method. A correctly configured NIP is critical for NTLM SSO to continue to function. **3. Which operating systems are vulnerable to this type of attack?** All versions of Windows that use NTLM are susceptible to this type of attack. Microsoft is releasing this new behavior only on the Windows 10 and Server 2016 platforms due to limitations in the older versions of the Windows Firewall, which preclude older operating systems from using this new behavior. Microsoft recommends customers upgrade to the newest, and most secure offerings. **4. Where can I find more information about Windows Information Protection?** See the following articles:		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	• Introducing Windows Information Protection • Protect your enterprise data using Windows Information Protection (WIP) **5. Where can I find details about enabling this functionality through Group Policy?** See https://technet.microsoft.com/en-us/library/jj865668(v=ws.10).aspx **6. Are there other ways to opt-in to this new behavior?** Yes. Both the Group Policy network isolation settings and Windows Information Protection cover the same area, both for Apps and for NTLM SSO Authentication. Using either is equally effective at mitigating NTLM SSO hash theft, but customers should select between these options. Mixing various means could create unexpected behavior. **7. Is a reboot required to enable this new behavior?** A reboot will be required to install the security update. When you then enable this new behavior with a Windows Registry change, the new behavior will be immediately take effect and not require a reboot. The changes to the Windows Firewall will have a varied delay depending on whether WIP or GP was used, and when this configuration is refreshed. **8. My enterprise has enabled this behavior, and now users are being prompted for credentials where they previously were not. Why is this happening?**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	This is an indication that the resource is marked as public or that its designation is uncertain, if the strictest mode has been enabled. This is most likely a symptom of the resource being inaccurately represented in your enterpriseâ€™s NIP, or you have configured 0 and the application is not using SMB, RPC, or HTTP. To check whether a resource is public, please enable the â€œNetwork Isolation Operationalâ€ logs under Windows Firewall with Advanced Security in Event Viewer. For the purposes of the log, enterprise resources are considered private. Please note that Network Isolation policies from Group Policy and WIP settings only affect networks whose profile is â€œDomainâ€. For more information about network profiles, please see: Understanding Firewall Profiles. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information Published.		

Affected Software

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

ADV170014						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4042895 Security Update			4038781	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 for x64-based Systems	4042895 Security Update			4038781	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1511 for x64-based Systems	4041689 Security Update			4038783	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1511 for 32-bit Systems	4041689 Security Update			4038783	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2016	4041691 Security Update			4038782	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV170014						
Windows 10 Version 1607 for 32-bit Systems	4041691 Security Update			4038782	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1607 for x64-based Systems	4041691 Security Update			4038782	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2016 (Server Core installation)	4041691 Security Update			4038782	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1703 for 32-bit Systems	4041676 Security Update			4038788	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1703 for x64-based Systems	4041676 Security Update			4038788	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV170016 - Windows Server 2008 Defense in Depth

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV170016 MITRE NVD	**CVE Title:** Windows Server 2008 Defense in Depth **Description:** Microsoft has released an update for Microsoft Windows Server 2008 that provides enhanced security as a defense-in-depth measure. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.	None	Defense in Depth

Affected Software

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

ADV170016						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4042723 Security Update	None	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Maybe
Windows Server 2008 for 32-bit Systems Service Pack 2	4042723 Security Update	None	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Maybe
Windows Server 2008 for x64-based Systems Service Pack 2	4042723 Security Update	None	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Maybe
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4042723 Security Update	None	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Maybe

ADV170017 - Office Defense in Depth Update

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV170017 MITRE NVD	**CVE Title:** Office Defense in Depth Update **Description:** Microsoft has released an update for Microsoft Office that provides enhanced security as a defense-in-depth measure. **FAQ:** **How should this update be deployed?** The update can be applied from Microsoft Update or the Download Center to existing Office installations by following the links in the KB articles listed in the Affected Products table. In addition, the update can be deployed in a new installation of Office by placing the Office setup files in the Updates folder in the Office installation image as follows: 1. Download OfficeSetupFiles.zip from the following link: OfficeSetupFiles. 2. Extract the files from OfficeSetupFiles.zip. There are x86 and x64 versions of OSE.EXE and OSETUP.DLL for Office 2010, Office 2013, and Office 2016.	None	Defense in Depth

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	3. Copy the files for the appropriate Office version and architecture into the Updates folder in the installation image. If the Updates folder already contains older versions of the same files, replace the old files with the new ones. 4. Install Office. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

ADV170017						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

ADV170017						
Microsoft Office 2010 Service Pack 2 (32-bit editions)	2553338 Security Update 2837599 Security Update	None	Defense in Depth	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	2553338 Security Update 2837599 Security Update	None	Defense in Depth	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (32-bit editions)	3172524 Security Update 3172531 Security Update	None	Defense in Depth	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (64-bit editions)	3172524 Security Update 3172531 Security Update	None	Defense in Depth	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 RT Service Pack 1	3172524 Security Update 3172531 Security	None	Defense in Depth	None	Base: N/A Temporal:	Maybe

ADV170017						
	Update				N/A Vector: N/A	
Microsoft Office 2016 (32-bit edition)	2920723 Security Update 4011185 Security Update	None	Defense in Depth	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	2920723 Security Update 4011185 Security Update	None	Defense in Depth	None	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-11762 - Microsoft Graphics Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11762 MITRE NVD	**CVE Title:** Microsoft Graphics Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. An attacker who successfully exploited the 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 click a link in an email or instant message that	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	takes users to the attacker's website, or by opening an attachment sent through email. • In a file-sharing attack scenario, an attacker could provide a specially crafted document file designed to exploit the vulnerability and then convince users to open the document file. The security update addresses the vulnerability by correcting how the Windows font library handles embedded fonts. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11762						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Critical	Remote Code Execution	4038777	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Critical	Remote Code Execution	4038777	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11762						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4041678 Security Only 4041681 Monthly Rollup	Critical	Remote Code Execution	4038777	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Critical	Remote Code Execution	4038777	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4041678 Security Only 4041681 Monthly	Critical	Remote Code Execution	4038777	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11762						
Service Pack 1	Rollup					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4042122 Security Update	Critical	Remote Code Execution	4038777	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe
Windows Server 2012	4041679 Security Only 4041690 Monthly Rollup	Critical	Remote Code Execution	4038799	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4041679 Security Only 4041690 Monthly	Critical	Remote Code Execution	4038799	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11762						
	Rollup					
Windows 8.1 for 32-bit systems	4041687 Security Only 4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4041687 Security Only 4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4041687 Security Only 4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11762						
Windows RT 8.1	4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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)	4041687 Security Only 4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11762						
x64-based Systems						
Windows 10 Version 1511 for 32-bit Systems	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11762						
Windows Server 2016 (Server Core installation)	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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	4042122 Security Update	Critical	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe

CVE-2017-11762						
Windows Server 2008 for 32-bit Systems Service Pack 2	4042122 Security Update	Critical	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for x64-based Systems Service Pack 2	4042122 Security Update	Critical	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4042122 Security Update	Critical	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe

CVE-2017-11763 - Microsoft Graphics Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11763 MITRE NVD	**CVE Title:** Microsoft Graphics Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. An attacker who successfully exploited the 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 click a link in an email or instant message that	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	takes users to the attacker's website, or by opening an attachment sent through email. • In a file-sharing attack scenario, an attacker could provide a specially crafted document file designed to exploit the vulnerability and then convince users to open the document file. The security update addresses the vulnerability by correcting how the Windows font library handles embedded fonts. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11763						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Critical	Remote Code Execution	4038777	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Critical	Remote Code Execution	4038777	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11763						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4041678 Security Only 4041681 Monthly Rollup	Critical	Remote Code Execution	4038777	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Critical	Remote Code Execution	4038777	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4041678 Security Only 4041681 Monthly	Critical	Remote Code Execution	4038777	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11763						
Service Pack 1	Rollup					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4042122 Security Update	Critical	Remote Code Execution	4038777	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe
Windows Server 2012	4041679 Security Only 4041690 Monthly Rollup	Critical	Remote Code Execution	4038799	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4041679 Security Only 4041690 Monthly	Critical	Remote Code Execution	4038799	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11763						
	Rollup					
Windows 8.1 for 32-bit systems	4041687 Security Only 4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4041687 Security Only 4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4041687 Security Only 4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11763						
Windows RT 8.1	4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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)	4041687 Security Only 4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11763						
x64-based Systems						
Windows 10 Version 1511 for 32-bit Systems	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11763						
Windows Server 2016 (Server Core installation)	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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	4042122 Security Update	Critical	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe

CVE-2017-11763						
Windows Server 2008 for 32-bit Systems Service Pack 2	4042122 Security Update	Critical	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for x64-based Systems Service Pack 2	4042122 Security Update	Critical	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4042122 Security Update	Critical	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe

CVE-2017-11765 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11765 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system. The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11765						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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-	4041678 Security	Important	Information Disclosure	4038777	Base: 5.5 Temporal: 5	Yes

CVE-2017-11765						
based Systems Service Pack 1	Only 4041681 Monthly Rollup				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11765						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4042120 Security Update	Important	Information Disclosure	4038777	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Maybe
Windows Server 2012	4041679 Security Only 4041690 Monthly	Important	Information Disclosure	4038799	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11765						
	Rollup					
Windows Server 2012 (Server Core installation)	4041679 Security Only 4041690 Monthly Rollup	Important	Information Disclosure	4038799	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4041687 Security Only 4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4041687 Security Only 4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11765						
Windows Server 2012 R2	4041687 Security Only 4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4041687 Security Only 4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4042895 Security Update	Important	Information Disclosure	4038781	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11765						
Windows 10 for x64-based Systems	4042895 Security Update	Important	Information Disclosure	4038781	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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 1511 for x64-based Systems	4041689 Security Update	Important	Information Disclosure	4038783	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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 1511 for 32-bit Systems	4041689 Security Update	Important	Information Disclosure	4038783	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4041691 Security Update	Important	Information Disclosure	4038782	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4041691 Security Update	Important	Information Disclosure	4038782	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11765						
Windows 10 Version 1607 for x64-based Systems	4041691 Security Update	Important	Information Disclosure	4038782	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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)	4041691 Security Update	Important	Information Disclosure	4038782	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4041676 Security Update	Important	Information Disclosure	4038788	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4041676 Security Update	Important	Information Disclosure	4038788	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4042120 Security	Important	Information Disclosure	4038788	Base: 5.5 Temporal: 5	Maybe

CVE-2017-11765						
2008 for Itanium-Based Systems Service Pack 2	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2	4042120 Security Update	Important	Information Disclosure	4038788	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for x64-based Systems Service Pack 2	4042120 Security Update	Important	Information Disclosure	4038788	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for	4042120 Security	Important	Information Disclosure	4038788	Base: 5.5 Temporal: 5	Maybe

CVE-2017-11765						
x64-based Systems Service Pack 2 (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	

CVE-2017-11769 - TRIE Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11769 MITRE NVD	**CVE Title:** TRIE Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that certain Windows components handle the loading of DLL files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11769						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-11769						
Windows 10 for 32-bit Systems	4042895 Security Update	Important	Remote Code Execution	4038781	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4042895 Security Update	Important	Remote Code Execution	4038781	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4041689 Security Update	Important	Remote Code Execution	4038783	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4041689 Security Update	Important	Remote Code Execution	4038783	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2016	4041691 Security Update	Important	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-11769						
Windows 10 Version 1607 for 32-bit Systems	4041691 Security Update	Important	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4041691 Security Update	Important	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4041691 Security Update	Important	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4041676 Security Update	Important	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4041676 Security Update	Important	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-11771 - Windows Search Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11771 MITRE NVD	**CVE Title:** Windows Search Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when Windows Search handles objects in memory. An attacker who successfully exploited this vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit the vulnerability, the attacker could send specially crafted messages to the Windows Search service. An attacker with access to a target computer could exploit this vulnerability to elevate privileges and take control of the computer. Additionally, in an enterprise scenario, a remote unauthenticated attacker could remotely trigger the vulnerability through an SMB connection and then take control of a target computer. The security update addresses the vulnerability by correcting how Windows Search handles objects in memory.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** **Disable WSearch service** Interactive workaround deployment steps 1. Click **Start**, click **Run**, type "regedit" (without the quotation marks), and then click **OK**. 2. Expand HKEY_LOCAL_MACHINE 3. Expand System, then CurrentControlSet, then Services 4. Click on **WSearch** 5. Click the **File** menu and select Export. 6. In the **Export Registry File** dialog type â€œWSearch_configuration_backup.regâ€□ and press **Save**. 7. Double-click the value named **Start** and change the **Value** data field to 4 8. Click **OK**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	9. Run the following command at a command prompt running as an administrator: **sc stop WSearch** Impact of workaround The Windows Search functionality will not be available to applications that use it for searches. How do undo the workaround 1. Click **Start** , click **Run** , type "regedit " (without the quotation marks), and then click **OK**. 2. Click the **File** menu and select Import. 3. In the **Import Registry File** dialog select â€œWSearch_configuration_backup.regâ€□ and press **Open**. Managed workaround deployment steps 1. First a backup copy of the registry keys can be made from a managed deployment script with the following command: **regedit /e WSearch_configuration_backup.reg HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WSearch**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	2. Next save the following to a file with a .REG extension (e.g. Disable_WSearch.reg) **Windows Registry Editor Version 5.00** **[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WSearch]** **"Start"=dword:00000004** 3. Run the registry script created in step 2 on the target machine with the following command: **regedit /s Disable_WSearch .reg** 4. Run the following command at a command prompt running as an administrator: **sc stop WSearch** Impact of workaround The Windows Search functionality will not be available to applications that use it for searches. How to undo the workaround Restore the original state by running the following command: **regedit /s WSearch_configuration_backup.reg** **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11771						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Critical	Remote Code Execution	4038777	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Critical	Remote Code Execution	4038777	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11771						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4041678 Security Only 4041681 Monthly Rollup	Critical	Remote Code Execution	4038777	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Critical	Remote Code Execution	4038777	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4041678 Security Only 4041681 Monthly	Critical	Remote Code Execution	4038777	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11771						
Service Pack 1	Rollup					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4042067 Security Update	Critical	Remote Code Execution	4038777	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe
Windows Server 2012	4041679 Security Only 4041690 Monthly Rollup	Critical	Remote Code Execution	4038799	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4041679 Security Only 4041690 Monthly	Critical	Remote Code Execution	4038799	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11771						
	Rollup					
Windows 8.1 for 32-bit systems	4041687 Security Only 4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4041687 Security Only 4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4041687 Security Only 4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11771						
Windows RT 8.1	4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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)	4041687 Security Only 4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11771						
x64-based Systems						
Windows 10 Version 1511 for 32-bit Systems	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11771						
Windows Server 2016 (Server Core installation)	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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	4042067 Security Update	Critical	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe

CVE-2017-11771						
Windows Server 2008 for 32-bit Systems Service Pack 2	4042067 Security Update	Critical	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for x64-based Systems Service Pack 2	4042067 Security Update	Critical	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4042067 Security Update	Critical	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe

CVE-2017-11772 - Microsoft Search Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11772 MITRE NVD	**CVE Title:** Microsoft Search Information Disclosure Vulnerability **Description:** An Information disclosure vulnerability exists when Windows Search improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. To exploit the vulnerability, the attacker could send specially crafted messages to the Windows Search service. Additionally, in an enterprise scenario, a remote unauthenticated attacker could trigger the vulnerability through an SMB connection. The security update addresses the vulnerability by correcting how Windows Search handles objects in memory. **FAQ:** None	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** **Disable WSearch service** Interactive workaround deployment steps 1. Click **Start**, click **Run**, type "regedit" (without the quotation marks), and then click **OK**. 2. Expand HKEY_LOCAL_MACHINE 3. Expand System, then CurrentControlSet, then Services 4. Click on **WSearch** 5. Click the **File** menu and select Export. 6. In the **Export Registry File** dialog type â€œWSearch_configuration_backup.regâ€□ and press **Save**. 7. Double-click the value named **Start** and change the **Value** data field to 4 8. Click **OK** 9. Run the following command at a command prompt running as an administrator: **sc stop WSearch** Impact of workaround		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The Windows Search functionality will not be available to applications that use it for searches. How do undo the workaround 1. Click **Start** , click **Run** , type "regedit " (without the quotation marks), and then click **OK**. 2. Click the **File** menu and select Import. 3. In the **Import Registry File** dialog select â€œWSearch_configuration_backup.regâ€ and press **Open**. Managed workaround deployment steps 1. First a backup copy of the registry keys can be made from a managed deployment script with the following command: **regedit /e WSearch_configuration_backup.reg HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WSearch** 2. Next save the following to a file with a .REG extension (e.g. Disable_WSearch.reg) **Windows Registry Editor Version 5.00** **[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WSearc**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	h] **"Start"=dword:00000004** 3. Run the registry script created in step 2 on the target machine with the following command: **regedit /s Disable_WSearch .reg** 4. Run the following command at a command prompt running as an administrator: **sc stop WSearch** Impact of workaround The Windows Search functionality will not be available to applications that use it for searches. How to undo the workaround Restore the original state by running the following command: **regedit /s WSearch_configuration_backup.reg** **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11772						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 5.9 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4041678 Security Only 4041681	Important	Information Disclosure	4038777	Base: 5.9 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes

CVE-2017-11772						
	Monthly Rollup					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 5.9 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4041678 Security Only 4041681 Monthly	Important	Information Disclosure	4038777	Base: 5.9 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes

CVE-2017-11772						
	Rollup					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4042067 Security Update	Important	Information Disclosure	4038777	Base: 5.9 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Maybe
Windows Server 2012	4041679 Security Only 4041690 Monthly Rollup	Important	Information Disclosure	4038799	Base: 5.9 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes

CVE-2017-11772						
Windows Server 2012 (Server Core installation)	4041679 Security Only 4041690 Monthly Rollup	Important	Information Disclosure	4038799	Base: 5.9 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4041687 Security Only 4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 5.9 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4041687 Security Only 404169	Important	Information Disclosure	4038792	Base: 5.9 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes

CVE-2017-11772						
	3 Monthly Rollup					
Windows Server 2012 R2	4041687 Security Only 4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 5.9 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows RT 8.1	4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 5.9 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core	4041687 Security Only 404169	Important	Information Disclosure	4038792	Base: 5.9 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes

CVE-2017-11772						
installation)	3 Monthly Rollup					
Windows 10 for 32-bit Systems	4042895 Security Update	Important	Information Disclosure	4038781	Base: 5.9 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4042895 Security Update	Important	Information Disclosure	4038781	Base: 5.9 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4041689 Security Update	Important	Information Disclosure	4038783	Base: 5.9 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows 10 Version 1511 for	4041689 Security	Important	Information Disclosure	4038783	Base: 5.9 Temporal: 5.7 Vector:	Yes

CVE-2017-11772						
32-bit Systems	Update				CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	
Windows Server 2016	4041691 Security Update	Important	Information Disclosure	4038782	Base: 5.9 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4041691 Security Update	Important	Information Disclosure	4038782	Base: 5.9 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4041691 Security Update	Important	Information Disclosure	4038782	Base: 5.9 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows Server 2016 (Server Core	4041691 Security Update	Important	Information Disclosure	4038782	Base: 5.9 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes

CVE-2017-11772						
installation)						
Windows 10 Version 1703 for 32-bit Systems	4041676 Security Update	Important	Information Disclosure	4038788	Base: 5.9 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4041676 Security Update	Important	Information Disclosure	4038788	Base: 5.9 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4042067 Security Update	Important	Information Disclosure	4038788	Base: 5.9 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Maybe
Windows Server 2008 for x64-based	4042067 Security	Important	Information Disclosure	4038788	Base: 5.9 Temporal: 5.7 Vector:	Maybe

CVE-2017-11772						
Systems Service Pack 2	Update				CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4042067 Security Update	Important	Information Disclosure	4038788	Base: 5.9 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Maybe

CVE-2017-11774 - Microsoft Outlook Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11774 MITRE NVD	**CVE Title:** Microsoft Outlook Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists when Microsoft Office improperly handles objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary commands. In a file-sharing attack scenario, an attacker could provide a specially crafted document file designed to exploit the vulnerability, and then convince users to open the document file and interact with the document. The security update addresses the vulnerability by correcting how Microsoft Office handles objects in memory. **FAQ:** None **Mitigations:** None	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11774						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Outlook 2013 RT Service Pack 1	4011178 Security Update	Important	Security Feature Bypass	4011090	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Outlook 2010 Service Pack 2 (32-bit editions)	4011196 Security Update	Important	Security Feature Bypass	4011089	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-11774						
Microsoft Outlook 2010 Service Pack 2 (64-bit editions)	4011196 Security Update	Important	Security Feature Bypass	4011089	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Outlook 2016 (32-bit edition)	4011162 Security Update	Important	Security Feature Bypass	4011091	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Outlook 2016 (64-bit edition)	4011162 Security Update	Important	Security Feature Bypass	4011091	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Outlook 2013 Service Pack 1 (32-bit editions)	4011178 Security Update	Important	Security Feature Bypass	4011090	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Outlook 2013 Service Pack 1 (64-bit editions)	4011178 Security Update	Important	Security Feature Bypass	4011090	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-11775 - Microsoft Office SharePoint XSS Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11775 MITRE NVD	**CVE Title:** Microsoft Office SharePoint XSS Vulnerability **Description:** A cross-site scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11775						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Enterprise Server 2016	4011157 Security Update	Important	Elevation of Privilege	4011127	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-11775						
Microsoft SharePoint Enterprise Server 2013 Service Pack 1	4011170 Security Update	Important	Elevation of Privilege	4011113	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-11776 - Microsoft Outlook Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11776 MITRE NVD	**CVE Title:** Microsoft Outlook Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Microsoft Outlook fails to establish a secure connection. An attacker who exploited the vulnerability could use it to obtain the email content of a user. The security update addresses the vulnerability by preventing Outlook from disclosing user email content.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11776						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Outlook 2016 (32-bit edition)	4011162 Security Update	Important	Information Disclosure	4011091	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-11776						
Microsoft Outlook 2016 (64-bit edition)	4011162 Security Update	Important	Information Disclosure	4011091	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-11777 - Microsoft Office SharePoint XSS Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11777 MITRE NVD	**CVE Title:** Microsoft Office SharePoint XSS Vulnerability **Description:** A cross-site scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11777						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Enterprise Server 2016	4011157 Security Update	Important	Elevation of Privilege	4011127	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2013 Service Pack 1	4011170 Security Update	Important	Elevation of Privilege	4011113	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-11779 - Windows DNSAPI Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11779	**CVE Title:** Windows DNSAPI Remote Code Execution Vulnerability **Description:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A remote code execution vulnerability exists in Windows Domain Name System (DNS) DNSAPI.dll when it fails to properly handle DNS responses. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the Local System Account. To exploit the vulnerability, the attacker would use a malicious DNS server to send corrupted DNS responses to the target. The update addresses the vulnerability by modifying how Windows DNSAPI.dll handles DNS responses. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11779						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012	4041679 Security Only 4041690 Monthly Rollup	Critical	Remote Code Execution	4038799	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4041679 Security Only 4041690 Monthly Rollup	Critical	Remote Code Execution	4038799	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11779						
Windows 8.1 for 32-bit systems	4041687 Security Only 4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4041687 Security Only 4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4041687 Security Only 4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11779						
Windows RT 8.1	4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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)	4041687 Security Only 4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11779						
x64-based Systems						
Windows 10 Version 1511 for 32-bit Systems	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11779						
Windows Server 2016 (Server Core installation)	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11780 - Windows SMB Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11780 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 1.0 (SMBv1) 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 SMBv1 server. The security update addresses the vulnerability by correcting how SMBv1 handles these specially crafted requests. **FAQ:** None **Mitigations:** **Workarounds:** None	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11780						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Remote Code Execution	4038777	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based	4041678 Security Only	Important	Remote Code Execution	4038777	Base: 8.1 Temporal: 7.3	Yes

CVE-2017-11780						
Systems Service Pack 1	4041681 Monthly Rollup				Vector: CVSS:3.0/AV:N/AC:H/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 (Server Core installation)	4041678 Security Only 4041681 Monthly Rollup	Important	Remote Code Execution	4038777	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Remote Code Execution	4038777	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11780						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Remote Code Execution	4038777	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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)	4041995 Security Update	Important	Remote Code Execution	4038777	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe
Windows Server 2012	4041679 Security Only 4041690 Monthly	Important	Remote Code Execution	4038799	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11780						
	Rollup					
Windows Server 2012 (Server Core installation)	4041679 Security Only 4041690 Monthly Rollup	Important	Remote Code Execution	4038799	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4041687 Security Only 4041693 Monthly Rollup	Important	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4041687 Security Only 4041693 Monthly Rollup	Important	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11780						
Windows Server 2012 R2	4041687 Security Only 4041693 Monthly Rollup	Important	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4041693 Monthly Rollup	Important	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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)	4041687 Security Only 4041693 Monthly Rollup	Important	Remote Code Execution	4038792	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4042895 Security Update	Important	Remote Code Execution	4038781	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11780						
Windows 10 for x64-based Systems	4042895 Security Update	Important	Remote Code Execution	4038781	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4041689 Security Update	Important	Remote Code Execution	4038783	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4041689 Security Update	Important	Remote Code Execution	4038783	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4041691 Security Update	Important	Remote Code Execution	4038782	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4041691 Security Update	Important	Remote Code Execution	4038782	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11780						
Windows 10 Version 1607 for x64-based Systems	4041691 Security Update	Important	Remote Code Execution	4038782	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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)	4041691 Security Update	Important	Remote Code Execution	4038782	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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	4041676 Security Update	Important	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/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	4041676 Security Update	Important	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11780						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4041995 Security Update	Important	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for 32-bit Systems Service Pack 2	4041995 Security Update	Important	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for x64-based Systems Service Pack 2	4041995 Security Update	Important	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe

CVE-2017-11780						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4041995 Security Update	Important	Remote Code Execution	4038788	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe

CVE-2017-11781 - Windows SMB Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11781 MITRE NVD	**CVE Title:** Windows SMB Denial of Service Vulnerability **Description:** A denial of service vulnerability exists in the Microsoft Server Block Message (SMB) when an attacker sends specially crafted requests to the server. An attacker who exploited this	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	vulnerability could cause the affected system to crash. To attempt to exploit this issue, an attacker would need to send specially crafted SMB requests to the target system. Note that the denial of service vulnerability would not allow an attacker to execute code or to elevate their user rights, but it could cause the affected system to stop accepting requests. The security update addresses the vulnerability by correcting the manner in which SMB handles specially crafted client requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11781						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Denial of Service	4038777	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Denial of Service	4038777	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-11781						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4041678 Security Only 4041681 Monthly Rollup	Important	Denial of Service	4038777	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Denial of Service	4038777	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems	4041678 Security Only 4041681 Monthly	Important	Denial of Service	4038777	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-11781						
Service Pack 1	Rollup					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4041995 Security Update	Important	Denial of Service	4038777	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Maybe
Windows Server 2012	4041679 Security Only 4041690 Monthly Rollup	Important	Denial of Service	4038799	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4041679 Security Only 4041690 Monthly	Important	Denial of Service	4038799	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-11781						
	Rollup					
Windows 8.1 for 32-bit systems	4041687 Security Only 4041693 Monthly Rollup	Important	Denial of Service	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4041687 Security Only 4041693 Monthly Rollup	Important	Denial of Service	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4041687 Security Only 4041693 Monthly Rollup	Important	Denial of Service	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-11781						
Windows RT 8.1	4041693 Monthly Rollup	Important	Denial of Service	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4041687 Security Only 4041693 Monthly Rollup	Important	Denial of Service	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4042895 Security Update	Important	Denial of Service	4038781	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4042895 Security Update	Important	Denial of Service	4038781	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-	4041689 Security Update	Important	Denial of Service	4038783	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-11781						
based Systems						
Windows 10 Version 1511 for 32-bit Systems	4041689 Security Update	Important	Denial of Service	4038783	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2016	4041691 Security Update	Important	Denial of Service	4038782	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4041691 Security Update	Important	Denial of Service	4038782	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4041691 Security Update	Important	Denial of Service	4038782	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4041691 Security Update	Important	Denial of Service	4038782	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-11781						
Windows 10 Version 1703 for 32-bit Systems	4041676 Security Update	Important	Denial of Service	4038788	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4041676 Security Update	Important	Denial of Service	4038788	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4041995 Security Update	Important	Denial of Service	4038788	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for 32-bit Systems Service Pack 2	4041995 Security Update	Important	Denial of Service	4038788	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Maybe

CVE-2017-11781						
Windows Server 2008 for x64-based Systems Service Pack 2	4041995 Security Update	Important	Denial of Service	4038788	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4041995 Security Update	Important	Denial of Service	4038788	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Maybe

CVE-2017-11782 - Windows SMB Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11782 MITRE NVD	**CVE Title:** Windows SMB Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the default Windows SMB Server configuration which allows anonymous users to remotely access certain named pipes that are also configured to allow anonymous access to users who are logged on locally. An unauthenticated attacker who successfully exploits this configuration error could remotely send specially crafted requests to certain services that accept requests via named pipes. To exploit the vulnerability, an attacker would have to be able to send SMB messages to an impacted Windows SMB Server for which the attacker does not already have valid credentials, and then identify an unpatched vulnerability in the handling of named pipe requests in one of the impacted services. The update addresses the vulnerability by correcting the Windows SMB Server default configuration. **FAQ:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11782						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2016	4041691 Security Update	Important	Elevation of Privilege	4038782	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-2017-11782						
Windows 10 Version 1607 for 32-bit Systems	4041691 Security Update	Important	Elevation of Privilege	4038782	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	4041691 Security Update	Important	Elevation of Privilege	4038782	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)	4041691 Security Update	Important	Elevation of Privilege	4038782	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-2017-11783 - Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11783 MITRE NVD	**CVE Title:** Windows Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC). An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control over an affected system. The update addresses the vulnerability by correcting how Windows handles calls to ALPC. **FAQ:** None **Mitigations:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11783						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 8.1 for 32-bit systems	4041687 Security Only 4041693 Monthly Rollup	Important	Elevation of Privilege	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11783						
Windows 8.1 for x64-based systems	4041687 Security Only 4041693 Monthly Rollup	Important	Elevation of Privilege	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4041687 Security Only 4041693 Monthly Rollup	Important	Elevation of Privilege	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4041693 Monthly Rollup	Important	Elevation of Privilege	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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)	4041687 Security Only 4041693 Monthly	Important	Elevation of Privilege	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11783						
	Rollup					
Windows 10 for 32-bit Systems	4042895 Security Update	Important	Elevation of Privilege	4038781	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4042895 Security Update	Important	Elevation of Privilege	4038781	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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 1511 for x64-based Systems	4041689 Security Update	Important	Elevation of Privilege	4038783	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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 1511 for 32-bit Systems	4041689 Security Update	Important	Elevation of Privilege	4038783	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4041691 Security	Important	Elevation of Privilege	4038782	Base: 7 Temporal: 6.3	Yes

CVE-2017-11783						
	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 1607 for 32-bit Systems	4041691 Security Update	Important	Elevation of Privilege	4038782	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4041691 Security Update	Important	Elevation of Privilege	4038782	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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)	4041691 Security Update	Important	Elevation of Privilege	4038782	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4041676 Security Update	Important	Elevation of Privilege	4038788	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11783						
Windows 10 Version 1703 for x64-based Systems	4041676 Security Update	Important	Elevation of Privilege	4038788	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11784 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11784 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object. To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11784						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-11784						
Windows 7 for 32-bit Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041678 Security Only 404168	Important	Information Disclosure	4038777	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11784						
Service Pack 1 (Server Core installation)	1 Monthly Rollup					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041678 Security Only 4041681 Monthly	Important	Information Disclosure	4038777	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11784						
	Rollup					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4041671 Security Update	Important	Information Disclosure	None	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041679 Security Only 4041690 Monthly Rollup	Important	Information Disclosure	4038799	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11784						
Windows Server 2012 (Server Core installation)	4041679 Security Only 4041690 Monthly Rollup	Important	Information Disclosure	4038799	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041687 Security Only 4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041687 Security Only 404169	Important	Information Disclosure	4038792	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11784						
	3 Monthly Rollup					
Windows Server 2012 R2	4041687 Security Only 4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041687 Security Only 404169	Important	Information Disclosure	4038792	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11784						
installation)	3 Monthly Rollup					
Windows 10 for 32-bit Systems	4042895 Security Update	Important	Information Disclosure	4038781	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4042895 Security Update	Important	Information Disclosure	4038781	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041671 Security Update	Important	Information Disclosure	None	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11784						
Windows Server 2008 for 32-bit Systems Service Pack 2	4041671 Security Update	Important	Information Disclosure	None	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041671 Security Update	Important	Information Disclosure	None	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041671 Security Update	Important	Information Disclosure	None	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11784						
installation)						

CVE-2017-11785 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11785 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object. To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses. **FAQ:** None **Mitigations:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11785						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4041678 Security Only 4041681	Important	Information Disclosure	4038777	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11785						
	Monthly Rollup					
Windows 7 for x64-based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11785						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041671 Security Update	Important	Information Disclosure	None	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11785						
Service Pack 2 (Server Core installation)						
Windows Server 2012	4041679 Security Only 4041690 Monthly Rollup	Important	Information Disclosure	4038799	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4041679 Security Only 4041690 Monthly	Important	Information Disclosure	4038799	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11785						
	Rollup					
Windows 8.1 for 32-bit systems	4041687 Security Only 4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041687 Security Only 4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041687 Security	Important	Information Disclosure	4038792	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2017-11785						
	Only 4041693 Monthly Rollup				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows RT 8.1	4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4041687 Security Only 4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4042895 Security	Important	Information Disclosure	4038781	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2017-11785						
	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 for x64-based Systems	4042895 Security Update	Important	Information Disclosure	4038781	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1511 for x64-based Systems	4041689 Security Update	Important	Information Disclosure	4038783	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1511 for 32-bit Systems	4041689 Security Update	Important	Information Disclosure	4038783	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041691 Security Update	Important	Information Disclosure	4038782	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11785						
Windows 10 Version 1607 for 32-bit Systems	4041691 Security Update	Important	Information Disclosure	4038782	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041691 Security Update	Important	Information Disclosure	4038782	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4041691 Security Update	Important	Information Disclosure	4038782	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041676 Security Update	Important	Information Disclosure	4038788	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11785						
Windows 10 Version 1703 for x64-based Systems	4041676 Security Update	Important	Information Disclosure	4038788	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041671 Security Update	Important	Information Disclosure	None	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041671 Security Update	Important	Information Disclosure	None	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041671 Security	Important	Information Disclosure	None	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2017-11785						
x64-based Systems Service Pack 2	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4041671 Security Update	Important	Information Disclosure	None	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11786 - Skype for Business Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11786 MITRE NVD	**CVE Title:** Skype for Business Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Skype for Business fails to properly handle specific authentication requests. An authenticated attacker who successfully exploited this vulnerability could steal an authentication hash that can be reused elsewhere. The attacker could then take any action that the user had permissions for, causing possible outcomes that could vary between users. To exploit the vulnerability, an attacker could invite a user to an instant message session while using a malicious profile image. The security update addresses the vulnerability by correcting how Skype for Business handles authentication requests. **FAQ:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11786						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Lync 2013 Service Pack 1 (32-bit)	4011179 Security Update	Important	Elevation of Privilege	4011107	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-11786						
Microsoft Lync 2013 Service Pack 1 (64-bit)	4011179 Security Update	Important	Elevation of Privilege	4011107	Base: N/A Temporal: N/A Vector: N/A	Maybe
Skype for Business 2016 (32-bit)	4011159 Security Update	Important	Elevation of Privilege	4011040	Base: N/A Temporal: N/A Vector: N/A	Maybe
Skype for Business 2016 (64-bit)	4011159 Security Update	Important	Elevation of Privilege	4011040	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-11790 - Internet Explorer Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11790	**CVE Title:** Internet Explorer Information Disclosure Vulnerability **Description:**	Low	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	An information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. To exploit the vulnerability, in a web-based attack scenario, an attacker could host a website 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 modifying how Internet Explorer handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11790						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems	4040685 IE Cumulative	Low	Information Disclosure	4036586	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-2017-11790						
Service Pack 2						
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4040685 IE Cumulative	Low	Information Disclosure	4036586	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 for 32-bit Systems Service Pack 1	4041681 Monthly Rollup 4040685 IE Cumulative	Important	Information Disclosure	4036586	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-2017-11790						
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4041681 Monthly Rollup 4040685 IE Cumulative	Important	Information Disclosure	4036586	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	4041681 Monthly Rollup 4040685 IE Cumulative	Low	Information Disclosure	4036586	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-2017-11790						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4041693 Monthly Rollup 4040685 IE Cumulative	Important	Information Disclosure	4036586	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	4041693 Monthly Rollup 4040685 IE Cumulative	Important	Information Disclosure	4036586	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	4041693 Monthly Rollup 4040685 IE Cumulative	Low	Information Disclosure	4036586	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-2017-11790						
Internet Explorer 11 on Windows RT 8.1	4041693 Monthly Rollup	Important	Information Disclosure	4038792	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	4042895 Security Update	Important	Information Disclosure	4038781	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	4042895 Security Update	Important	Information Disclosure	4038781	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	4041689 Security	Important	Information Disclosure	4038783	Base: 4.3 Temporal: 3.9 Vector:	Yes

CVE-2017-11790						
Windows 10 Version 1511 for x64-based Systems	Update				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 1511 for 32-bit Systems	4041689 Security Update	Important	Information Disclosure	4038783	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	4041691 Security Update	Low	Information Disclosure	4038782	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-2017-11790						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4041691 Security Update	Important	Information Disclosure	4038782	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 1607 for x64-based Systems	4041691 Security Update	Important	Information Disclosure	4038782	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 Window	4041676 Security Update	Important	Information Disclosure	4038788	Base: 4.3 Temporal: 3.9 Vector:	Yes

CVE-2017-11790						
s 10 Version 1703 for 32-bit Systems					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 1703 for x64-based Systems	4041676 Security Update	Important	Information Disclosure	4038788	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	4041690 Monthly Rollup 4040685 IE Cumulative	Low	Information Disclosure	4036586	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-2017-11792 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11792 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 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 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11792						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10	4041676 Security	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11792						
Version 1703 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 1703 for x64-based Systems	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11793 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11793 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11793						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-11793						
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	4040685 IE Cumulative	Moderate	Remote Code Execution	4036586	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4040685 IE Cumulative	Moderate	Remote Code Execution	4036586	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11793						
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4041681 Monthly Rollup 4040685 IE Cumulative	Critical	Remote Code Execution	4036586	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4041681 Monthly Rollup 4040685 IE Cumulative	Critical	Remote Code Execution	4036586	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4041681 Monthly Rollup 4040685 IE	Moderate	Remote Code Execution	4036586	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11793						
Server 2008 R2 for x64-based Systems Service Pack 1	Cumulative					
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4041693 Monthly Rollup 4040685 IE Cumulative	Critical	Remote Code Execution	4036586	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4041693 Monthly Rollup 4040685 IE Cumulative	Critical	Remote Code Execution	4036586	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11793						
Internet Explorer 11 on Windows Server 2012 R2	4041693 Monthly Rollup 4040685 IE Cumulative	Moderate	Remote Code Execution	4036586	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows RT 8.1	4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11793						
x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11793						
Internet Explorer 11 on Windows Server 2016	4041691 Security Update	Moderate	Remote Code Execution	4038782	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for x64-	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11793						
based Systems						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11793						
Internet Explorer 10 on Windows Server 2012	4041690 Monthly Rollup 4040685 IE Cumulative	Moderate	Remote Code Execution	4036586	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11794 - Microsoft Edge Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11794 MITRE NVD	**CVE Title:** Microsoft Edge Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Microsoft Edge improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. To exploit the vulnerability, in a web-based attack scenario, an attacker could host a website 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	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 update addresses the vulnerability by modifying how Microsoft Edge handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11794						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4041676 Security Update	Important	Information Disclosure	4038788	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	4041676 Security Update	Important	Information Disclosure	4038788	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-2017-11796 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11796 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 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 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11796						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10	4041676 Security	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11796						
Version 1703 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 1703 for x64-based Systems	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11797 - Scripting Engine Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11797 MITRE NVD	**CVE Title:** Scripting Engine Information Disclosure Vulnerability **Description:** A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how the ChakraCore scripting engine handles objects in memory. **FAQ:** None **Mitigations:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11797						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
ChakraCore	Commit Security Update	Critical	Remote Code Execution		Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11798 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11798 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 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 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11798						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows	4042895 Security	Critical	Remote Code Execution	4038781	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11798						
10 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 for x64-based Systems	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1511 for x64-based Systems	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1511 for 32-bit Systems	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11798						
Microsoft Edge on Windows Server 2016	4041691 Security Update	Moderate	Remote Code Execution	4038782	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/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	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11798						
1703 for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11799 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11799 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	Critical	Remote Code Execution

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11799						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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-	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11799						
based Systems						
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1511 for 32-bit Systems	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4041691 Security Update	Moderate	Remote Code Execution	4038782	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4041691 Security	Critical	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11799						
10 Version 1607 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 1607 for x64-based Systems	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11799						
x64-based Systems						
ChakraCore	Commit Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11800 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11800 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11800						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11800						
1511 for x64-based Systems						
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4041691 Security Update	Moderate	Remote Code Execution	4038782	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/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	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11800						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11801 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11801 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how the ChakraCore scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11801						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
ChakraCore	Commit Security Update	Critical	Remote Code Execution		Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11802 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11802 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11802						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1511 for	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11802						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4041691 Security Update	Moderate	Remote Code Execution	4038782	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/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	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4041691 Security	Critical	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11802						
10 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	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11804 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11804 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 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 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11804						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows	4042895 Security	Critical	Remote Code Execution	4038781	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11804						
10 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 for x64-based Systems	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1511 for x64-based Systems	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1511 for 32-bit Systems	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11804						
Microsoft Edge on Windows Server 2016	4041691 Security Update	Moderate	Remote Code Execution	4038782	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/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	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11804						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11805 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
11805 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 update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11805						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11805						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11806 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11806	**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	Critical	Remote Code Execution

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11806						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11806						
1703 for x64-based Systems						
ChakraCore	Commit Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11807 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11807 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11807						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11807						
	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	

CVE-2017-11808 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11808 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11808						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1511 for x64-based Systems	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4041689 Security	Critical	Remote Code Execution	4038783	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11808						
10 Version 1511 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 Server 2016	4041691 Security Update	Moderate	Remote Code Execution	4038782	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/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	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11808						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11809 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11809 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way the scripting engine handle objects in memory in Microsoft browsers. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website designed to exploit the vulnerability through a Microsoft browser and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the browser rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11809						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-11809						
Microsoft Edge on Windows 10 for 32-bit Systems	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1511 for x64-based Systems	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1511 for	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11809						
32-bit Systems						
Microsoft Edge on Windows Server 2016	4041691 Security Update	Moderate	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4041676 Security	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11809						
10 Version 1703 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 1703 for x64-based Systems	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11810 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11810 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11810						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-11810						
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	4040685 IE Cumulative	Moderate	Remote Code Execution	4036586	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4040685 IE Cumulative	Moderate	Remote Code Execution	4036586	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-2017-11810						
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4041681 Monthly Rollup 4040685 IE Cumulative	Critical	Remote Code Execution	4036586	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4041681 Monthly Rollup 4040685 IE Cumulative	Critical	Remote Code Execution	4036586	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4041681 Monthly Rollup 4040685 IE	Moderate	Remote Code Execution	4036586	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-2017-11810						
Server 2008 R2 for x64-based Systems Service Pack 1	Cumulative					
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4041693 Monthly Rollup 4040685 IE Cumulative	Critical	Remote Code Execution	4036586	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4041693 Monthly Rollup 4040685 IE Cumulative	Critical	Remote Code Execution	4036586	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11810						
Internet Explorer 11 on Windows Server 2012 R2	4041693 Monthly Rollup 4040685 IE Cumulative	Moderate	Remote Code Execution	4036586	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	4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11810						
x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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 1511 for 32-bit Systems	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11810						
Internet Explorer 11 on Windows Server 2016	4041691 Security Update	Moderate	Remote Code Execution	4038782	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	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for x64-	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11810						
based Systems						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11810						
Internet Explorer 10 on Windows Server 2012	4041690 Monthly Rollup 4040685 IE Cumulative	Moderate	Remote Code Execution	4036586	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-2017-11811 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11811 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11811						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1511 for	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11811						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4041691 Security Update	Moderate	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4041691 Security	Critical	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11811						
10 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	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11812 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11812 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 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 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11812						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows	4041689 Security	Critical	Remote Code Execution	4038783	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11812						
10 Version 1511 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 1511 for 32-bit Systems	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4041691 Security Update	Moderate	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11812						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11812						
ChakraCore	Commit Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11813 - Internet Explorer Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11813 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	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	could also take advantage of compromised websites, or websites that accept or host user-provided content or advertisements, by adding specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action, typically by an enticement in an email or instant message, or by getting the user to open an attachment sent through email. The security update addresses the vulnerability by modifying how Internet Explorer handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11813						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4041681 Monthly Rollup 4040685 IE Cumulative	Critical	Remote Code Execution	4036586	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4041681 Monthly Rollup 4040685 IE Cumulative	Critical	Remote Code Execution	4036586	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11813						
Systems Service Pack 1						
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4041681 Monthly Rollup 4040685 IE Cumulative	Moderate	Remote Code Execution	4036586	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4041693 Monthly Rollup 4040685 IE Cumulative	Critical	Remote Code Execution	4036586	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11813						
Internet Explorer 11 on Windows 8.1 for x64-based systems	4041693 Monthly Rollup 4040685 IE Cumulative	Critical	Remote Code Execution	4036586	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4041693 Monthly Rollup 4040685 IE Cumulative	Moderate	Remote Code Execution	4036586	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	4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11814 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11814 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system. The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11814						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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-	4041678 Security	Important	Information Disclosure	4038777	Base: 5.5 Temporal: 5	Yes

CVE-2017-11814						
based Systems Service Pack 1	Only 4041681 Monthly Rollup				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11814						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4042120 Security Update	Important	Information Disclosure	4038777	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Maybe
Windows Server 2012	4041679 Security Only 4041690 Monthly	Important	Information Disclosure	4038799	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11814						
	Rollup					
Windows Server 2012 (Server Core installation)	4041679 Security Only 4041690 Monthly Rollup	Important	Information Disclosure	4038799	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4041687 Security Only 4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4041687 Security Only 4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11814						
Windows Server 2012 R2	4041687 Security Only 4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4041687 Security Only 4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4042895 Security Update	Important	Information Disclosure	4038781	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11814						
Windows 10 for x64-based Systems	4042895 Security Update	Important	Information Disclosure	4038781	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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 1511 for x64-based Systems	4041689 Security Update	Important	Information Disclosure	4038783	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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 1511 for 32-bit Systems	4041689 Security Update	Important	Information Disclosure	4038783	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4041691 Security Update	Important	Information Disclosure	4038782	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4041691 Security Update	Important	Information Disclosure	4038782	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11814						
Windows 10 Version 1607 for x64-based Systems	4041691 Security Update	Important	Information Disclosure	4038782	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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)	4041691 Security Update	Important	Information Disclosure	4038782	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4041676 Security Update	Important	Information Disclosure	4038788	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4041676 Security Update	Important	Information Disclosure	4038788	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4042120 Security	Important	Information Disclosure	4038788	Base: 5.5 Temporal: 5	Maybe

CVE-2017-11814						
2008 for Itanium-Based Systems Service Pack 2	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2	4042120 Security Update	Important	Information Disclosure	4038788	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for x64-based Systems Service Pack 2	4042120 Security Update	Important	Information Disclosure	4038788	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for	4042120 Security	Important	Information Disclosure	4038788	Base: 5.5 Temporal: 5	Maybe

CVE-2017-11814						
x64-based Systems Service Pack 2 (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	

CVE-2017-11815 - Windows SMB Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11815 MITRE NVD	**CVE Title:** Windows SMB Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests. An authenticated attacker who successfully exploited this vulnerability could craft a special packet, which could lead to information disclosure from the server.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, an attacker would have to be able to authenticate and send SMB messages to an impacted Windows SMB Server The security update addresses the vulnerability by correcting how Windows SMB Server handles authenticated requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11815						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-11815						
(Server Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems	4041995 Security Update	Important	Information Disclosure	4038777	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Maybe

CVE-2017-11815						
Service Pack 2 (Server Core installation)						
Windows Server 2012	4041679 Security Only 4041690 Monthly Rollup	Important	Information Disclosure	4038799	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4041679 Security Only 4041690 Monthly Rollup	Important	Information Disclosure	4038799	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4041687 Security Only 4041693	Important	Information Disclosure	4038792	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-11815						
	Monthly Rollup					
Windows 8.1 for x64-based systems	4041687 Security Only 4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server	4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-11815						
Core installation)						
Windows 10 for 32-bit Systems	4042895 Security Update	Important	Information Disclosure	4038781	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4042895 Security Update	Important	Information Disclosure	4038781	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4041689 Security Update	Important	Information Disclosure	4038783	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4041689 Security Update	Important	Information Disclosure	4038783	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2016	4041691 Security	Important	Information Disclosure	4038782	Base: 6.4 Temporal: 5.8	Yes

CVE-2017-11815						
	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	
Windows 10 Version 1607 for 32-bit Systems	4041691 Security Update	Important	Information Disclosure	4038782	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4041691 Security Update	Important	Information Disclosure	4038782	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4041691 Security Update	Important	Information Disclosure	4038782	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4041676 Security Update	Important	Information Disclosure	4038788	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-11815						
Windows 10 Version 1703 for x64-based Systems	4041676 Security Update	Important	Information Disclosure	4038788	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4041995 Security Update	Important	Information Disclosure	4038788	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for 32-bit Systems Service Pack 2	4041995 Security Update	Important	Information Disclosure	4038788	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for	4041995 Security	Important	Information Disclosure	4038788	Base: 6.4 Temporal: 5.8	Maybe

CVE-2017-11815						
x64-based Systems Service Pack 2	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4041995 Security Update	Important	Information Disclosure	4038788	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	Maybe

CVE-2017-11816 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11816 MITRE NVD	**CVE Title:** Windows GDI Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system. By itself, the information disclosure does not allow arbitrary code execution; however, it could allow arbitrary code to be run if the attacker uses it in combination with another vulnerability. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how GDI handles memory addresses. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11816						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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-	4041678 Security	Important	Information Disclosure	4038777	Base: 5.5 Temporal: 5	Yes

CVE-2017-11816						
based Systems Service Pack 1	Only 4041681 Monthly Rollup				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11816						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4042121 Security Update	Important	Information Disclosure	4038777	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Maybe
Windows Server 2012	4041679 Security Only 4041690 Monthly	Important	Information Disclosure	4038799	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11816						
	Rollup					
Windows Server 2012 (Server Core installation)	4041679 Security Only 4041690 Monthly Rollup	Important	Information Disclosure	4038799	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4041687 Security Only 4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4041687 Security Only 4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11816						
Windows Server 2012 R2	4041687 Security Only 4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4041687 Security Only 4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4042895 Security Update	Important	Information Disclosure	4038781	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11816						
Windows 10 for x64-based Systems	4042895 Security Update	Important	Information Disclosure	4038781	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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 1511 for x64-based Systems	4041689 Security Update	Important	Information Disclosure	4038783	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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 1511 for 32-bit Systems	4041689 Security Update	Important	Information Disclosure	4038783	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4041691 Security Update	Important	Information Disclosure	4038782	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4041691 Security Update	Important	Information Disclosure	4038782	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11816						
Windows 10 Version 1607 for x64-based Systems	4041691 Security Update	Important	Information Disclosure	4038782	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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)	4041691 Security Update	Important	Information Disclosure	4038782	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4041676 Security Update	Important	Information Disclosure	4038788	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4041676 Security Update	Important	Information Disclosure	4038788	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4042121 Security	Important	Information Disclosure	4038788	Base: 5.5 Temporal: 5	Maybe

CVE-2017-11816						
2008 for Itanium-Based Systems Service Pack 2	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2	4042121 Security Update	Important	Information Disclosure	4038788	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for x64-based Systems Service Pack 2	4042121 Security Update	Important	Information Disclosure	4038788	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for	4042121 Security	Important	Information Disclosure	4038788	Base: 5.5 Temporal: 5	Maybe

CVE-2017-11816						
x64-based Systems Service Pack 2 (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	

CVE-2017-11817 - Windows Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11817 MITRE NVD	**CVE Title:** Windows Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory. To exploit this vulnerability, an authenticated attacker could run a specially crafted application. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The update addresses the vulnerability by correcting how the Windows kernel initializes objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11817						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-11817						
Windows 7 for 32-bit Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041678 Security Only 404168	Important	Information Disclosure	4038777	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11817						
Service Pack 1 (Server Core installation)	1 Monthly Rollup					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Information Disclosure	4038777	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041678 Security Only 4041681 Monthly	Important	Information Disclosure	4038777	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11817						
	Rollup					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4041944 Security Update	Important	Information Disclosure	4038777	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Maybe
Windows Server 2012	4041679 Security Only 4041690 Monthly Rollup	Important	Information Disclosure	4038799	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11817						
Windows Server 2012 (Server Core installation)	4041679 Security Only 4041690 Monthly Rollup	Important	Information Disclosure	4038799	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041687 Security Only 4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041687 Security Only 404169	Important	Information Disclosure	4038792	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11817						
	3 Monthly Rollup					
Windows Server 2012 R2	4041687 Security Only 4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041693 Monthly Rollup	Important	Information Disclosure	4038792	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041687 Security Only 404169	Important	Information Disclosure	4038792	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11817						
installation)	3 Monthly Rollup					
Windows 10 for 32-bit Systems	4042895 Security Update	Important	Information Disclosure	4038781	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4042895 Security Update	Important	Information Disclosure	4038781	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1511 for x64-based Systems	4041689 Security Update	Important	Information Disclosure	4038783	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1511 for	4041689 Security	Important	Information Disclosure	4038783	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2017-11817						
32-bit Systems	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2016	4041691 Security Update	Important	Information Disclosure	4038782	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041691 Security Update	Important	Information Disclosure	4038782	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041691 Security Update	Important	Information Disclosure	4038782	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041691 Security Update	Important	Information Disclosure	4038782	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11817						
installation)						
Windows 10 Version 1703 for 32-bit Systems	4041676 Security Update	Important	Information Disclosure	4038788	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041676 Security Update	Important	Information Disclosure	4038788	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4041944 Security Update	Important	Information Disclosure	4038788	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for	4041944 Security	Important	Information Disclosure	4038788	Base: 4.7 Temporal: 4.2 Vector:	Maybe

CVE-2017-11817						
32-bit Systems Service Pack 2	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2	4041944 Security Update	Important	Information Disclosure	4038788	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4041944 Security Update	Important	Information Disclosure	4038788	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Maybe

CVE-2017-11818 - Windows Storage Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11818 MITRE NVD	**CVE Title:** Windows Storage Security Feature Bypass Vulnerability **Description:** An Security Feature bypass vulnerability exists in Microsoft Windows storage when it fails to validate an integrity-level check. An attacker who successfully exploited the vulnerability could allow an application with a certain integrity level to execute code at a different integrity level. The update addresses the vulnerability by correcting how Microsoft storage validates an integrity-level check. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11818						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012	4041679 Security Only 4041690 Monthly Rollup	Important	Security Feature Bypass	4038799	Base: 4.5 Temporal: 4.1 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2012	4041679 Security Only	Important	Security Feature Bypass	4038799	Base: 4.5 Temporal: 4.1	Yes

CVE-2017-11818						
(Server Core installation)	4041690 Monthly Rollup				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4041687 Security Only 4041693 Monthly Rollup	Important	Security Feature Bypass	4038792	Base: 4.5 Temporal: 4.1 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4041687 Security Only 4041693 Monthly Rollup	Important	Security Feature Bypass	4038792	Base: 4.5 Temporal: 4.1 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4041687 Security Only 4041693 Monthly	Important	Security Feature Bypass	4038792	Base: 4.5 Temporal: 4.1 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-11818						
	Rollup					
Windows RT 8.1	4041693 Monthly Rollup	Important	Security Feature Bypass	4038792	Base: 4.5 Temporal: 4.1 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4041687 Security Only 4041693 Monthly Rollup	Important	Security Feature Bypass	4038792	Base: 4.5 Temporal: 4.1 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4042895 Security Update	Important	Security Feature Bypass	4038781	Base: 4.5 Temporal: 4.1 Vector: CVSS:3.0/AV:L/AC:H/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	4042895 Security Update	Important	Security Feature Bypass	4038781	Base: 4.5 Temporal: 4.1 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-11818						
Windows 10 Version 1511 for x64-based Systems	4041689 Security Update	Important	Security Feature Bypass	4038783	Base: 4.5 Temporal: 4.1 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4041689 Security Update	Important	Security Feature Bypass	4038783	Base: 4.5 Temporal: 4.1 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2016	4041691 Security Update	Important	Security Feature Bypass	4038782	Base: 4.5 Temporal: 4.1 Vector: CVSS:3.0/AV:L/AC:H/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	4041691 Security Update	Important	Security Feature Bypass	4038782	Base: 4.5 Temporal: 4.1 Vector: CVSS:3.0/AV:L/AC:H/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	4041691 Security Update	Important	Security Feature Bypass	4038782	Base: 4.5 Temporal: 4.1 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-11818						
Windows Server 2016 (Server Core installation)	4041691 Security Update	Important	Security Feature Bypass	4038782	Base: 4.5 Temporal: 4.1 Vector: CVSS:3.0/AV:L/AC:H/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	4041676 Security Update	Important	Security Feature Bypass	4038788	Base: 4.5 Temporal: 4.1 Vector: CVSS:3.0/AV:L/AC:H/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	4041676 Security Update	Important	Security Feature Bypass	4038788	Base: 4.5 Temporal: 4.1 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-11819 - Windows Shell Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-	**CVE Title:** Windows Shell Remote Code Execution Vulnerability **Description:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
11819 MITRE NVD	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory. The vulnerability could corrupt memory in a way that could allow an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, the attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. An attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft browsers, and then convince a user to view the website. The attacker could also take advantage of compromised websites, or websites that accept or host user-provided content or advertisements, by adding specially crafted content that could exploit the vulnerability. In all cases, however, an attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically via an enticement in email or instant message, or by getting them to open an email attachment. The update addresses the vulnerability by modifying how Microsoft browsers handle objects in memory. **FAQ:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11819						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4041678 Security Only 4041681 Monthly	Critical	Remote Code Execution	4038777	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11819						
	Rollup					
Windows 7 for x64-based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Critical	Remote Code Execution	4038777	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11820 - Microsoft Office SharePoint XSS Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11820 MITRE NVD	**CVE Title:** Microsoft Office SharePoint XSS Vulnerability **Description:** A cross-site scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11820						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Enterprise Server 2016	4011157 Security Update	Important	Elevation of Privilege	4011127	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2013 Service Pack 1	4011180 Security Update	Important	Elevation of Privilege	4011117	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-11821 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11821 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 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 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11821						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10	4041676 Security	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11821						
Version 1703 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 1703 for x64-based Systems	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Update	Critical	Remote Code Execution	4038788	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11822 - Internet Explorer Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11822 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 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11822						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-11822						
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	4040685 IE Cumulative	Moderate	Remote Code Execution	4036586	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4040685 IE Cumulative	Moderate	Remote Code Execution	4036586	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-2017-11822						
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4041681 Monthly Rollup 4040685 IE Cumulative	Critical	Remote Code Execution	4036586	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4041681 Monthly Rollup 4040685 IE Cumulative	Critical	Remote Code Execution	4036586	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4041681 Monthly Rollup 4040685 IE	Moderate	Remote Code Execution	4036586	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-2017-11822						
Server 2008 R2 for x64-based Systems Service Pack 1	Cumulative					
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4041693 Monthly Rollup 4040685 IE Cumulative	Critical	Remote Code Execution	4036586	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4041693 Monthly Rollup 4040685 IE Cumulative	Critical	Remote Code Execution	4036586	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11822						
Internet Explorer 11 on Windows Server 2012 R2	4041693 Monthly Rollup 4040685 IE Cumulative	Moderate	Remote Code Execution	4036586	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	4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11822						
x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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 1511 for 32-bit Systems	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11822						
Internet Explorer 11 on Windows Server 2016	4041691 Security Update	Moderate	Remote Code Execution	4038782	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	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for x64-	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11822						
based Systems						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11823 - Microsoft Windows Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11823 MITRE NVD	**CVE Title:** Microsoft Windows Security Feature Bypass **Description:** A security feature bypass vulnerability exists in Device Guard that could allow an attacker to inject malicious code into a Windows PowerShell session. An attacker who successfully exploited this vulnerability could inject code into a trusted PowerShell process to bypass the Device Guard Code Integrity policy on the local machine. To exploit the vulnerability, an attacker would first have to access the local machine, and then inject malicious code into a script that is trusted by the Code Integrity policy. The injected code would then run with the same trust level as the script and bypass the Code Integrity policy. The update addresses the vulnerability by correcting how PowerShell exposes functions and processes user supplied code. **FAQ:** None **Mitigations:** None	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11823						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4042895 Security Update	Important	Security Feature Bypass	4038781	Base: 6.3 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H	Yes
Windows 10 for x64-based Systems	4042895 Security Update	Important	Security Feature Bypass	4038781	Base: 6.3 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H	Yes

CVE-2017-11823						
Windows 10 Version 1511 for x64-based Systems	4041689 Security Update	Important	Security Feature Bypass	4038783	Base: 6.3 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H	Yes
Windows 10 Version 1511 for 32-bit Systems	4041689 Security Update	Important	Security Feature Bypass	4038783	Base: 6.3 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H	Yes
Windows Server 2016	4041691 Security Update	Important	Security Feature Bypass	4038782	Base: 6.3 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H	Yes
Windows 10 Version 1607 for 32-bit Systems	4041691 Security Update	Important	Security Feature Bypass	4038782	Base: 6.3 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H	Yes
Windows 10 Version 1607 for x64-based Systems	4041691 Security Update	Important	Security Feature Bypass	4038782	Base: 6.3 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H	Yes
Windows Server 2016 (Server Core installation)	4041691 Security	Important	Security Feature Bypass	4038782	Base: 6.3 Temporal: 6.3	Yes

CVE-2017-11823						
	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H	
Windows 10 Version 1703 for 32-bit Systems	4041676 Security Update	Important	Security Feature Bypass	4038788	Base: 6.3 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H	Yes
Windows 10 Version 1703 for x64-based Systems	4041676 Security Update	Important	Security Feature Bypass	4038788	Base: 6.3 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H	Yes

CVE-2017-11824 - Windows Graphics Component Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11824	**CVE Title:** Windows Graphics Component Elevation of Privilege Vulnerability **Description:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run processes in an elevated context. In a local attack scenario, an attacker could exploit this vulnerability by running a specially crafted application to take control over the affected system. The update addresses the vulnerability by correcting the way in which the Microsoft Graphics Component handles objects in memory and preventing unintended elevation from user mode. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11824						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Elevation of Privilege	4038777	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Elevation of Privilege	4038777	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11824						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4041678 Security Only 4041681 Monthly Rollup	Important	Elevation of Privilege	4038777	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Elevation of Privilege	4038777	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4041678 Security Only 4041681 Monthly	Important	Elevation of Privilege	4038777	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11824						
Service Pack 1	Rollup					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4042120 Security Update	Important	Elevation of Privilege	4038777	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe
Windows Server 2012	4041679 Security Only 4041690 Monthly Rollup	Important	Elevation of Privilege	4038799	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4041679 Security Only 4041690 Monthly	Important	Elevation of Privilege	4038799	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11824						
	Rollup					
Windows 8.1 for 32-bit systems	4041687 Security Only 4041693 Monthly Rollup	Important	Elevation of Privilege	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4041687 Security Only 4041693 Monthly Rollup	Important	Elevation of Privilege	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4041687 Security Only 4041693 Monthly Rollup	Important	Elevation of Privilege	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11824						
Windows RT 8.1	4041693 Monthly Rollup	Important	Elevation of Privilege	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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)	4041687 Security Only 4041693 Monthly Rollup	Important	Elevation of Privilege	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4042895 Security Update	Important	Elevation of Privilege	4038781	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4042895 Security Update	Important	Elevation of Privilege	4038781	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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 1511 for	4041689 Security Update	Important	Elevation of Privilege	4038783	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11824						
x64-based Systems						
Windows 10 Version 1511 for 32-bit Systems	4041689 Security Update	Important	Elevation of Privilege	4038783	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4041691 Security Update	Important	Elevation of Privilege	4038782	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4041691 Security Update	Important	Elevation of Privilege	4038782	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4041691 Security Update	Important	Elevation of Privilege	4038782	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11824						
Windows Server 2016 (Server Core installation)	4041691 Security Update	Important	Elevation of Privilege	4038782	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4041676 Security Update	Important	Elevation of Privilege	4038788	Base: 0 Temporal: 0 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4041676 Security Update	Important	Elevation of Privilege	4038788	Base: 0 Temporal: 0 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4042120 Security Update	Important	Elevation of Privilege	4038788	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe

CVE-2017-11824						
Windows Server 2008 for 32-bit Systems Service Pack 2	4042120 Security Update	Important	Elevation of Privilege	4038788	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for x64-based Systems Service Pack 2	4042120 Security Update	Important	Elevation of Privilege	4038788	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4042120 Security Update	Important	Elevation of Privilege	4038788	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe

CVE-2017-11825 - Microsoft Office Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11825 MITRE NVD	**CVE Title:** Microsoft Office Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when it fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could use a specially crafted file to perform actions in the security context of the current user. For example, the file could then take actions on behalf of the logged-on user with the same permissions as the current user. To exploit the vulnerability, a user must open a specially crafted file with an affected version of Microsoft Office software. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) that contains a specially crafted file that is designed to exploit the vulnerability. However, an attacker would have no way to force the user to visit the website. Instead, an attacker would have to convince the user to click a link, typically by way of an	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	enticement in an email or Instant Messenger message, and then convince the user to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Office handles files in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11825						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2016 for Mac	Release Notes Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions	Click to Run Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-11826 - Microsoft Office Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11826 MITRE NVD	**CVE Title:** Microsoft Office Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office software. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Office handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11826						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Word 2007 Service Pack 3	3213648 Security Update	Important	Remote Code Execution	3203441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (32-bit editions)	3213630 Security Update 3213627 Security Update	Important	Remote Code Execution	3203463	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft Word 2010 Service Pack 2 (64-bit editions)	3213630 Security Update 3213627 Security Update	Important	Remote Code Execution	3203463	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft Word 2013 Service Pack 1 (32-bit editions)	4011232 Security Update	Important	Remote Code Execution	3203393	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (64-bit editions)	4011232 Security Update	Important	Remote Code Execution	3203393	Base: N/A Temporal:	Maybe

CVE-2017-11826						
					N/A Vector: N/A	
Microsoft Word 2013 RT Service Pack 1	4011232 Security Update	Important	Remote Code Execution	3203393	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Web Apps Server 2013 Service Pack 1	4011231 Security Update	Important	Remote Code Execution	3213562	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Web Apps Server 2010 Service Pack 2	4011194 Security Update	Important	Remote Code Execution	3213632	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2016 (32-bit edition)	4011222 Security Update	Important	Remote Code Execution	3191945	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2016 (64-bit edition)	4011222 Security Update	Important	Remote Code Execution	3191945	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-11826						
Microsoft Office Online Server 2016	3213659 Security Update	Important	Remote Code Execution	3213658	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4011217 Security Update	Important	Remote Code Execution	4011127	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Word Viewer	4011236 Security Update	Important	Remote Code Execution	3191909	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Compatibility Pack Service Pack 3	3213647 Security Update	Important	Remote Code Execution	3203438	Base: N/A Temporal: N/A Vector: N/A	Maybe
Word Automation Services on Microsoft SharePoint Server 2010 Service Pack 2	3213623 Security Update	Important	Remote Code Execution	3203458	Base: N/A Temporal: N/A Vector: N/A	Maybe
Word Automation Services on Microsoft SharePoint Server 2013 Service Pack 1	4011068 Security Update	Important	Remote Code Execution	3203384	Base: N/A Temporal:	Maybe

CVE-2017-11826						
					N/A Vector: N/A	

CVE-2017-11829 - Windows Update Delivery Optimization Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11829 MITRE NVD	**CVE Title:** Windows Update Delivery Optimization Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows Update Delivery Optimization does not properly enforce file share permissions. An attacker who successfully exploited the vulnerability could overwrite files that require higher privileges than what the attacker already has. To exploit this vulnerability, an attacker would need to log into a system. The attacker could then create a Delivery Optimization job to exploit the vulnerability. The security update addresses the vulnerability by correcting how the Delivery Optimization services enforces permissions.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-11829						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2016	4041691 Security	Important	Elevation of Privilege	4038782	Base: 5.5 Temporal: 5	Yes

CVE-2017-11829						
	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1607 for 32-bit Systems	4041691 Security Update	Important	Elevation of Privilege	4038782	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4041691 Security Update	Important	Elevation of Privilege	4038782	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4041691 Security Update	Important	Elevation of Privilege	4038782	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4041676 Security Update	Important	Elevation of Privilege	4038788	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11829						
Windows 10 Version 1703 for x64-based Systems	4041676 Security Update	Important	Elevation of Privilege	4038788	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8689 - Win32k Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8689 MITRE NVD	**CVE Title:** Win32k Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows kernel-mode driver fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application to take control of an affected system.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The update addresses the vulnerability by correcting how the Windows kernel-mode driver handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-8689						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8689						
Windows 7 for 32-bit Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Elevation of Privilege	4038777	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Elevation of Privilege	4038777	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Elevation of Privilege	4038777	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8689						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Elevation of Privilege	4038777	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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)	4042120 Security Update	Important	Elevation of Privilege	4038777	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe
Windows 8.1 for 32-bit systems	4041687 Security Only 4041693 Monthly Rollup	Important	Elevation of Privilege	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8689						
Windows 8.1 for x64-based systems	4041687 Security Only 4041693 Monthly Rollup	Important	Elevation of Privilege	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4041687 Security Only 4041693 Monthly Rollup	Important	Elevation of Privilege	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4041693 Monthly Rollup	Important	Elevation of Privilege	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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)	4041687 Security Only 4041693 Monthly	Important	Elevation of Privilege	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8689						
	Rollup					
Windows 10 for 32-bit Systems	4042895 Security Update	Important	Elevation of Privilege	4038781	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4042895 Security Update	Important	Elevation of Privilege	4038781	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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 1511 for x64-based Systems	4041689 Security Update	Important	Elevation of Privilege	4038783	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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 1511 for 32-bit Systems	4041689 Security Update	Important	Elevation of Privilege	4038783	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4041691 Security	Important	Elevation of Privilege	4038782	Base: 7 Temporal: 6.3	Yes

CVE-2017-8689						
	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 1607 for 32-bit Systems	4041691 Security Update	Important	Elevation of Privilege	4038782	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4041691 Security Update	Important	Elevation of Privilege	4038782	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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)	4041691 Security Update	Important	Elevation of Privilege	4038782	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4041676 Security Update	Important	Elevation of Privilege	4038788	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8689						
Windows 10 Version 1703 for x64-based Systems	4041676 Security Update	Important	Elevation of Privilege	4038788	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4042120 Security Update	Important	Elevation of Privilege	4038788	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for 32-bit Systems Service Pack 2	4042120 Security Update	Important	Elevation of Privilege	4038788	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for x64-based Systems	4042120 Security Update	Important	Elevation of Privilege	4038788	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe

CVE-2017-8689						
Service Pack 2						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4042120 Security Update	Important	Elevation of Privilege	4038788	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe

CVE-2017-8693 - Microsoft Graphics Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8693 MITRE NVD	**CVE Title:** Microsoft Graphics Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. 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 the way in which the Windows Graphics Component handles objects in memory. **FAQ:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-8693						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4042895 Security Update	Important	Information Disclosure	4038781	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8693						
Windows 10 for x64-based Systems	4042895 Security Update	Important	Information Disclosure	4038781	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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 1511 for x64-based Systems	4041689 Security Update	Important	Information Disclosure	4038783	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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 1511 for 32-bit Systems	4041689 Security Update	Important	Information Disclosure	4038783	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4041691 Security Update	Important	Information Disclosure	4038782	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4041691 Security Update	Important	Information Disclosure	4038782	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8693						
Windows 10 Version 1607 for x64-based Systems	4041691 Security Update	Important	Information Disclosure	4038782	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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)	4041691 Security Update	Important	Information Disclosure	4038782	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4041676 Security Update	Important	Information Disclosure	4038788	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/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	4041676 Security Update	Important	Information Disclosure	4038788	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8694 - Win32k Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8694 MITRE NVD	**CVE Title:** Win32k Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows kernel-mode driver fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application to take control of an affected system. The update addresses the vulnerability by correcting how the Windows kernel-mode driver handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-8694						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Elevation of Privilege	4038777	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8694						
Windows 7 for x64-based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Elevation of Privilege	4038777	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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)	4041678 Security Only 4041681 Monthly Rollup	Important	Elevation of Privilege	4038777	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4041678 Security Only 4041681 Monthly	Important	Elevation of Privilege	4038777	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8694						
Service Pack 1	Rollup					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Elevation of Privilege	4038777	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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)	4042120 Security Update	Important	Elevation of Privilege	4038777	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe
Windows Server 2012	4041679 Security Only 4041690 Monthly	Important	Elevation of Privilege	4038799	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8694						
	Rollup					
Windows Server 2012 (Server Core installation)	4041679 Security Only 4041690 Monthly Rollup	Important	Elevation of Privilege	4038799	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4041687 Security Only 4041693 Monthly Rollup	Important	Elevation of Privilege	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4041687 Security Only 4041693 Monthly Rollup	Important	Elevation of Privilege	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8694						
Windows Server 2012 R2	4041687 Security Only 4041693 Monthly Rollup	Important	Elevation of Privilege	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4041693 Monthly Rollup	Important	Elevation of Privilege	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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)	4041687 Security Only 4041693 Monthly Rollup	Important	Elevation of Privilege	4038792	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4042895 Security Update	Important	Elevation of Privilege	4038781	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8694						
Windows 10 for x64-based Systems	4042895 Security Update	Important	Elevation of Privilege	4038781	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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 1511 for x64-based Systems	4041689 Security Update	Important	Elevation of Privilege	4038783	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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 1511 for 32-bit Systems	4041689 Security Update	Important	Elevation of Privilege	4038783	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4041691 Security Update	Important	Elevation of Privilege	4038782	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4041691 Security Update	Important	Elevation of Privilege	4038782	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8694						
Windows 10 Version 1607 for x64-based Systems	4041691 Security Update	Important	Elevation of Privilege	4038782	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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)	4041691 Security Update	Important	Elevation of Privilege	4038782	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4041676 Security Update	Important	Elevation of Privilege	4038788	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4041676 Security Update	Important	Elevation of Privilege	4038788	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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-	4042120 Security	Important	Elevation of Privilege	4038788	Base: 7 Temporal: 6.3	Maybe

CVE-2017-8694						
Based Systems Service Pack 2	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 2008 for 32-bit Systems Service Pack 2	4042120 Security Update	Important	Elevation of Privilege	4038788	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for x64-based Systems Service Pack 2	4042120 Security Update	Important	Elevation of Privilege	4038788	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe
Windows Server 2008 for x64-based Systems Service	4042120 Security Update	Important	Elevation of Privilege	4038788	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Maybe

CVE-2017-8694						
Pack 2 (Server Core installation)						

CVE-2017-8703 - Windows Subsystem for Linux Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8703 MITRE NVD	**CVE Title:** Windows Subsystem for Linux Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when Windows Subsystem for Linux improperly handles objects in memory. An attacker who successfully exploited this vulnerability could cause a denial of service against the local system. A attacker could exploit this vulnerability by running a specially crafted application. The update addresses the vulnerability by correcting how Windows Subsystem for Linux handles objects in memory.	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-8703						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1703 for	4041676 Security	Important	Denial of Service	4038788	Base: 5 Temporal: 4.3	Yes

CVE-2017-8703						
x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:R	

CVE-2017-8715 - Windows Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8715 MITRE NVD	**CVE Title:** Windows Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists in Device Guard that could allow an attacker to inject malicious code into a Windows PowerShell session. An attacker who successfully exploited this vulnerability could inject code into a trusted PowerShell process to bypass the Device Guard Code Integrity policy on the local machine. To exploit the vulnerability, an attacker would first have to access the local machine, and then inject malicious code into a script that is trusted by the Code Integrity policy. The injected code would then run with the same trust level as the script and bypass the Code Integrity policy. The update addresses the vulnerability by correcting how PowerShell exposes functions and processes user supplied code.	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-8715						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4042895 Security	Important	Security Feature Bypass	4038781	Base: 5.3 Temporal: 4.8	Yes

CVE-2017-8715						
	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 for x64-based Systems	4042895 Security Update	Important	Security Feature Bypass	4038781	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 1511 for x64-based Systems	4041689 Security Update	Important	Security Feature Bypass	4038783	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 1511 for 32-bit Systems	4041689 Security Update	Important	Security Feature Bypass	4038783	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	4041691 Security Update	Important	Security Feature Bypass	4038782	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	4041691 Security Update	Important	Security Feature Bypass	4038782	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-2017-8715						
Windows 10 Version 1607 for x64-based Systems	4041691 Security Update	Important	Security Feature Bypass	4038782	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)	4041691 Security Update	Important	Security Feature Bypass	4038782	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	4041676 Security Update	Important	Security Feature Bypass	4038788	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	4041676 Security Update	Important	Security Feature Bypass	4038788	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-2017-8717 - Microsoft JET Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8717 MITRE NVD	**CVE Title:** Microsoft JET Database Engine Remote Code Execution Vulnerability **Description:** A buffer overflow vulnerability exists in the Microsoft JET Database Engine that could allow remote code execution on an affected system. An attacker who successfully exploited this vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. To exploit the vulnerability, a user must open or preview a specially crafted Excel file while using an affected version of Microsoft Windows. In an email attack scenario, an attacker could exploit the vulnerability by sending a specially crafted Excel file to the user, and then convincing the user to open the file. The security update addresses the vulnerability by modifying how the Microsoft JET Database Engine handles objects in memory.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-8717						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems	4041678 Security Only	Important	Remote Code Execution	4038777	Base: 7.1 Temporal: 6.4	Yes

CVE-2017-8717						
Service Pack 1	4041681 Monthly Rollup				Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 7 for x64-based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Remote Code Execution	4038777	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/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)	4041678 Security Only 4041681 Monthly Rollup	Important	Remote Code Execution	4038777	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8717						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Remote Code Execution	4038777	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/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	4041678 Security Only 4041681 Monthly Rollup	Important	Remote Code Execution	4038777	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/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	4042007 Security Update	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8717						
Core installation)						
Windows Server 2012	4041679 Security Only 4041690 Monthly Rollup	Important	Remote Code Execution	4038799	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4041679 Security Only 4041690 Monthly Rollup	Important	Remote Code Execution	4038799	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4041687 Security Only 4041693 Monthly Rollup	Important	Remote Code Execution	4038792	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8717						
Windows 8.1 for x64-based systems	4041687 Security Only 4041693 Monthly Rollup	Important	Remote Code Execution	4038792	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4041687 Security Only 4041693 Monthly Rollup	Important	Remote Code Execution	4038792	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4041693 Monthly Rollup	Important	Remote Code Execution	4038792	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server	4041687 Security Only 4041693 Monthly	Important	Remote Code Execution	4038792	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8717						
Core installation)	Rollup					
Windows 10 for 32-bit Systems	4042895 Security Update	Important	Remote Code Execution	4038781	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4042895 Security Update	Important	Remote Code Execution	4038781	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4041689 Security Update	Important	Remote Code Execution	4038783	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4041689 Security Update	Important	Remote Code Execution	4038783	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4041691 Security	Important	Remote Code Execution	4038782	Base: 7.1 Temporal: 6.4	Yes

CVE-2017-8717						
	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1607 for 32-bit Systems	4041691 Security Update	Important	Remote Code Execution	4038782	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/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	4041691 Security Update	Important	Remote Code Execution	4038782	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4041691 Security Update	Important	Remote Code Execution	4038782	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/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	4041676 Security Update	Important	Remote Code Execution	4038788	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8717						
Windows 10 Version 1703 for x64-based Systems	4041676 Security Update	Important	Remote Code Execution	4038788	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/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	4042007 Security Update	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/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	4042007 Security Update	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for	4042007 Security	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.4	Yes

CVE-2017-8717						
x64-based Systems Service Pack 2	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4042007 Security Update	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8718 - Microsoft JET Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8718 MITRE NVD	**CVE Title:** Microsoft JET Database Engine Remote Code Execution Vulnerability **Description:** A buffer overflow vulnerability exists in the Microsoft JET Database Engine that could allow remote code execution on an affected system. An attacker who successfully exploited this vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. To exploit the vulnerability, a user must open or preview a specially crafted Excel file while using an affected version of Microsoft Windows. In an email attack scenario, an attacker could exploit the vulnerability by sending a specially crafted Excel file to the user, and then convincing the user to open the file. The security update addresses the vulnerability by modifying how the Microsoft JET Database Engine handles objects in memory.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-8718						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems	4041678 Security Only	Important	Remote Code Execution	4038777	Base: 7.1 Temporal: 6.4	Yes

CVE-2017-8718						
Service Pack 1	4041681 Monthly Rollup				Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 7 for x64-based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Remote Code Execution	4038777	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/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)	4041678 Security Only 4041681 Monthly Rollup	Important	Remote Code Execution	4038777	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8718						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Important	Remote Code Execution	4038777	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/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	4041678 Security Only 4041681 Monthly Rollup	Important	Remote Code Execution	4038777	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/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	4042007 Security Update	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8718						
Core installation)						
Windows Server 2012	4041679 Security Only 4041690 Monthly Rollup	Important	Remote Code Execution	4038799	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4041679 Security Only 4041690 Monthly Rollup	Important	Remote Code Execution	4038799	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4041687 Security Only 4041693 Monthly Rollup	Important	Remote Code Execution	4038792	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8718						
Windows 8.1 for x64-based systems	4041687 Security Only 4041693 Monthly Rollup	Important	Remote Code Execution	4038792	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4041687 Security Only 4041693 Monthly Rollup	Important	Remote Code Execution	4038792	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4041693 Monthly Rollup	Important	Remote Code Execution	4038792	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server	4041687 Security Only 4041693 Monthly	Important	Remote Code Execution	4038792	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8718						
Core installation)	Rollup					
Windows 10 for 32-bit Systems	4042895 Security Update	Important	Remote Code Execution	4038781	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4042895 Security Update	Important	Remote Code Execution	4038781	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4041689 Security Update	Important	Remote Code Execution	4038783	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4041689 Security Update	Important	Remote Code Execution	4038783	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4041691 Security	Important	Remote Code Execution	4038782	Base: 7.1 Temporal: 6.4	Yes

CVE-2017-8718						
	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1607 for 32-bit Systems	4041691 Security Update	Important	Remote Code Execution	4038782	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/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	4041691 Security Update	Important	Remote Code Execution	4038782	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4041691 Security Update	Important	Remote Code Execution	4038782	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/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	4041676 Security Update	Important	Remote Code Execution	4038788	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8718						
Windows 10 Version 1703 for x64-based Systems	4041676 Security Update	Important	Remote Code Execution	4038788	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/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	4042007 Security Update	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/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	4042007 Security Update	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for	4042007 Security	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.4	Yes

CVE-2017-8718						
x64-based Systems Service Pack 2	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4042007 Security Update	Important	Remote Code Execution	None	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8726 - Microsoft Edge Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8726 MITRE NVD	**CVE Title:** Microsoft Edge Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way affected Microsoft scripting engines render when handling 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 designed to exploit the vulnerability through Microsoft Edge 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 scripting rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by modifying how affected Microsoft scripting engines handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-8726						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8726						
Microsoft Edge on Windows 10 for 32-bit Systems	4042895 Security Update	Important	Information Disclosure	4038781	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 for x64-based Systems	4042895 Security Update	Important	Information Disclosure	4038781	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 1511 for x64-based Systems	4041689 Security Update	Important	Information Disclosure	4038783	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-2017-8726						
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4041689 Security Update	Important	Information Disclosure	4038783	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 2016	4041691 Security Update	Low	Information Disclosure	4038782	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 1607 for 32-bit Systems	4041691 Security Update	Important	Information Disclosure	4038782	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	4041691 Security	Important	Information Disclosure	4038782	Base: 4.3 Temporal: 3.9	Yes

CVE-2017-8726						
Windows 10 Version 1607 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 1703 for 32-bit Systems	4041676 Security Update	Important	Information Disclosure	4038788	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-	4041676 Security Update	Important	Information Disclosure	4038788	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-2017-8726						
based Systems						

CVE-2017-8727 - Windows Shell Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8727 MITRE NVD	**CVE Title:** Windows Shell Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory via the Microsoft Windows Text Services Framework. 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 an enticement in an email or instant message, or by getting them to open an attachment sent through email. The security update addresses the vulnerability by modifying how the Microsoft Windows Text Services Framework handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 10/10/2017 07:00:00 Information published.		

Affected Software

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

CVE-2017-8727						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Critical	Remote Code Execution	4038777	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4041678 Security Only 4041681 Monthly Rollup	Critical	Remote Code Execution	4038777	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8727						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4042123 Security Update	Critical	Remote Code Execution	4038777	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	Maybe
Windows Server 2012	4041679 Security Only 4041690 Monthly Rollup	Critical	Remote Code Execution	4038799	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4041679 Security Only 4041690 Monthly Rollup	Critical	Remote Code Execution	4038799	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-2017-8727						
Windows 8.1 for 32-bit systems	4041687 Security Only 4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4041687 Security Only 4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4041687 Security Only 4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	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-2017-8727						
Windows RT 8.1	4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4041687 Security Only 4041693 Monthly Rollup	Critical	Remote Code Execution	4038792	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4042895 Security Update	Critical	Remote Code Execution	4038781	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8727						
x64-based Systems						
Windows 10 Version 1511 for 32-bit Systems	4041689 Security Update	Critical	Remote Code Execution	4038783	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8727						
Windows Server 2016 (Server Core installation)	4041691 Security Update	Critical	Remote Code Execution	4038782	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4041676 Security Update	Critical	Remote Code Execution	4038788	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4042123 Security Update	Critical	Remote Code Execution	4038788	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	Maybe

CVE-2017-8727						
Windows Server 2008 for 32-bit Systems Service Pack 2	4042123 Security Update	Critical	Remote Code Execution	4038788	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	Maybe
Windows Server 2008 for x64-based Systems Service Pack 2	4042123 Security Update	Critical	Remote Code Execution	4038788	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	Maybe
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4042123 Security Update	Critical	Remote Code Execution	4038788	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	Maybe

声 明

==========

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。

关于绿盟科技

==========

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）成立于 2000 年 4 月，总部位于北京。在国内外设有 30 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测/防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易，股票简称：绿盟科技，股票代码：300369。

绿盟科技官方微博二维码

绿盟科技官方微信二维码