BD Product Name: BD EpiCenter

Date of Critical Security Patches: May 2019

Abstract: Critical security patches for May 2019

Microsoft® & Third-Party Patches

BD has identified patches from Microsoft® that have been identified as critical or security related for May 2019. These patches were not found to adversely affect BD products and will be applied according to customers' service agreement.

Customers that maintain patches independent of BD automated delivery should ensure the validated patches are installed on their BD systems as the acting responsible entity in order to maintain the correct security posture of the system(s).

Patch Name	Patch Description	Patch ID	Notes
03-2019 Service Stack update for Win7	This update makes quality improvements to the servicing stack component that installs Windows updates. Key changes include: • Addresses an issue in the servicing stack when you install an update that has been signed by using only the SHA-2 hash algorithm.	KB4490628	
03-2019 Security rollup for Win7	This security update includes quality improvements. No new operating system features are being introduced in this update. Key changes include: • Addresses an issue that causes the abbreviated Japanese Era names to be incorrect. For more information, see KB4469068. • Addresses an issue that may prevent the Event Viewer from showing some	KB4489885 KB4489878	

	event descriptions for network interface cards (NIC). • Security updates to Windows App Platform and Frameworks, Windows Cryptography, Windows Hyper-V, Windows Storage and Filesystems, Windows Fundamentals, Windows Server, Windows Kernel, Windows MSXML, and the Microsoft JET Database Engine.		
02-2019 Monthly Rollup for Win7	This security update includes quality improvements. No new operating system features are being introduced in this update. Key changes include: • Addresses an issue that may prevent applications that use a Microsoft Jet database with the Microsoft Access 97 file format from opening. This issue occurs if the database has column names greater than 32 characters. The database fails to open with the error, "Unrecognized Database Format". • Security updates to Windows App Platform and Frameworks, Windows Graphics, Windows Input and Composition, Windows Wireless Networking, Windows Server, and the Microsoft JET Database Engine	KB4486564	**1**
02-2019 Security Update	This update introduces SHA-2 code sign support for Windows 7 SP1, Windows Server 2008 R2 SP1, and Windows Server 2008 SP2.	KB4474419	**1**
12-2018 Cumulative security update for Internet Explorer for Win7	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. To learn more about the vulnerability, go to CVE-2018-8653.	KB4483187	**1**

11-2018 Security Update	This security update includes quality improvements. No new operating system features are being introduced in this update. Key changes include: • Security updates to Windows App Platform and Frameworks, Windows Graphics, Windows Wireless Networking, Windows Kernel, and Windows Server.	KB4467106	**1**
10-2018 Security Update	This security update includes quality improvements. No new operating system features are being introduced in this update. Key changes include: • Addresses an issue in which all guest virtual machines running Unicast NLB fail to respond to NLB requests after the virtual machines restart. • Security updates to Windows Media Player, Windows Graphics, Microsoft Graphics Component, Windows Storage and Filesystems, Windows Kernel, and the Microsoft JET Database Engine.	KB4462915	**1**
09-2018 Security Update	This security update includes quality improvements. No new operating system features are being introduced in this update. Key changes include: • Security updates to Windows media, Windows Shell, Windows Hyper-V, Windows kernel, Windows datacenter networking, Windows virtualization and kernel, Microsoft JET Database Engine, Windows MSXML, and Windows Server.	KB4457145	**1**
08-2018 Security Update	This security update includes quality improvements. No new operating system features are being introduced in this update. Key changes include: • Provides protections against a new speculative execution side-channel vulnerability known as L1 Terminal Fault (L1TF) that affects Intel® Core® processors and Intel® Xeon® processors (CVE-2018-3620 and CVE-2018-3646). Make sure previous OS protections against Spectre Variant 2 and Meltdown vulnerabilities are enabled using the registry settings outlined in the Windows Client and Windows Server guidance KB articles. (*These registry settings are enabled*	KB4343899	**1**

	by default for Windows Client OS editions, but disabled by default for Windows Server OS editions.) • Addresses an issue that causes high CPU usage that results in performance degradation on some systems with Family 15h and 16h AMD processors. This issue occurs after installing the June 2018 or July 2018 Windows updates from Microsoft and the AMD microcode updates that address Spectre Variant 2 (CVE-2017-5715 – Branch Target Injection). • Provides protections against an additional vulnerability involving side-channel speculative execution known as Lazy Floating Point (FP) State Restore (CVE-2018-3665) for 32-Bit (x86) versions of Windows.		
07-2018 Security Update	This security update includes quality improvements. No new operating system features are being introduced in this update. Key changes include: • Provides support to control use of Indirect Branch Prediction Barrier (IBPB) on some AMD processors (CPUs) for mitigating CVE-2017-5715, Spectre Variant 2 when switching from user context to kernel context. (See AMD Architecture Guidelines for Indirect Branch Control and AMD Security Updates for more details). For Windows client (IT pro) guidance, follow the instructions in KB4073119. For Windows Server guidance, follow the instructions in KB4072698. Use these guidance documents to enable use of IBPB on some AMD processors (CPUs) for mitigating Spectre Variant 2 when switching from user context to kernel context. • Provides protections from an additional subclass of speculative execution side channel vulnerability known as Speculative Store Bypass (CVE-2018-3639). These protections aren't enabled by default. For Windows client (IT pro) guidance, follow the instructions in KB4073119. For Windows Server guidance, follow the instructions in KB4072698. Use this guidance document to enable mitigations for Speculative Store Bypass (CVE-2018-3639) in addition to the mitigations that have	KB4284867	**1**

	already been released for Spectre Variant 2 (CVE-2017-5715) and Meltdown (CVE-2017-5754). • Security updates to Windows apps, Windows Server, Windows storage and filesystems, Windows wireless networking, and Windows virtualization and kernel.		
05-2018 Security Update	This security update includes quality improvements. No new operating system features are being introduced in this update. Key changes include: • Addresses an issue that may cause a memory leak on SMB servers after installing KB4056897 or any other recent monthly update. This leak may occur when the requested path traverses a symbolic link, a mount point, or a directory junction and the registry key is set to 1: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanManServer\Parameters\EnableEcp • Addresses an issue that may cause an error when connecting to a Remote Desktop server. For more information, see CredSSP updates for CVE-2018-0886. • Security updates to Internet Explorer, Windows apps, Windows kernel, Microsoft Graphics Component, Windows storage and filesystems, HTML help, and Windows Hyper-V.	KB4103712	**1**
04-2018 Security Update	This security update includes quality improvements. No new operating system features are being introduced in this update. Key changes include: • Windows Update and WSUS will offer this update to applicable Windows client and server operating systems, regardless of the existence or value of the "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\QualityCompat\cadca5fe-87d3-4b96-b7fb-a231484277cc" registry setting. This change has been made to protect user data. • Improves reliability in the kernel, and addresses an issue that can cause applications to have unexpected	KB4093108	**1**

	memory contents on multi-processor systems. • Addresses a stop error that occurred when the previous month's update was applied to a 32-bit (x86) computer with a Physical Address Extension (PAE) mode disabled. • Security updates to Internet Explorer, Microsoft scripting engine, Microsoft graphics component, Windows Server, Windows datacenter networking, Windows virtualization and kernel, and Windows app platform and frameworks.		
12-2017 Security Update	This security update includes improvements and fixes that were a part of update KB4051034 (released November 27, 2017) and addresses the following issues: • Addresses issue where users of SQL Server Reporting Services may not be able to use the scrollbar in a drop-down list. • Addresses additional issues with updated time zone information. • Security updates to the Microsoft Scripting Engine and Windows Server.	KB4054518	**1**
10-2017 Security Update	This security update includes quality improvements. No new operating system features are being introduced in this update. Key changes include: • Security updates to Microsoft Windows Search Component, Windows kernel-mode drivers, Microsoft Graphics Component, Internet Explorer, Windows kernel, Windows Wireless Networking, Microsoft JET Database Engine, and the Windows SMB Server.	KB4041678	**1**
09-2017 Security Update	This security update includes quality improvements. No new operating system features are being introduced in this update. Key changes include: • Addressed issue where UI elements, including menu bars, are missing from Windows and Java applications running on computers with multiple monitors (multimon). • Addressed issue where the WordPad application can sometimes crash on	KB4038779	**1**

	launch. The was a known issue first reported in KB4025337. • Re-release of MS16-087- Security update for Windows print spooler components. • Addressed issue where applications that have LDAP referral chasing options enabled use a TCP dynamic port connection that doesn't close until the applications close or the calling OS restarts. With sufficient time and volume, these applications may completely consume all TCP dynamic ports. If that occurs, network communications will fail for any protocol or operation that uses dynamic ports. This issue was introduced by the July and August 2017 cumulative updates, starting with KB4025337 and KB4025341.		
08-2017 Security Update	This security update includes quality improvements. No new operating system features are being introduced in this update. Key changes include: • Security updates to Windows Server, Microsoft JET Database Engine, Windows kernel-mode drivers, Common Log File System Driver, Microsoft Windows Search Component, and Volume Manager Driver.	KB4034679	**1**
07-2017 Security Update	This security update includes quality improvements. No new operating system features are being introduced in this update. Key changes include: • Security updates to Microsoft Graphics Component, Windows Search, Windows kernel-mode drivers, Windows Virtualization, Windows Server, Windows Storage and File Systems, Datacenter Networking, Windows shell, ASP.NET, Microsoft PowerShell, Windows kernel, and Microsoft NTFS.	KB4025337	**1**

06-2017 Security Update	This security update includes quality improvements. No new operating system features are being introduced in this update. Key changes include: • Addressed issue where, after installing KB3164035, users cannot print enhanced metafiles (EMF) or documents containing bitmaps rendered out of bounds using the **BitMapSection(DIBSection)** function. • Addressed issue where updates were not correctly installing all components and would prevent them from booting. • Addressed issue where an unsupported hardware notification is shown and Windows Updates not scanning, for systems using the AMD Carrizo DDR4 processor. For the affected systems, follow the steps in the Additional Information section to install this update. • Security updates to Windows kernel, Microsoft Graphics Component, Microsoft Uniscribe, Windows kernel-mode drivers, the Windows OS, Windows COM and Windows shell. For more information about the security vulnerabilities resolved, please refer to the Security Update Guide.	KB4022722	**1**
05-2017 Security Update	This security update includes quality improvements. No new operating system features are being introduced in this update. Key changes include: • Updated Windows Cryptography API to deprecate SHA-1 for SSL/TLS Server Authentication, including in Microsoft Edge and Internet Explorer 11 . See Advisory 4010323 for more information. • Security updates to Microsoft Graphics Component, Windows COM, Microsoft ActiveX, Windows Server, Windows kernel, and Microsoft Windows DNS.	KB4019263	**1**

04-2017 Security Update	This security update resolves security vulnerabilities in scripting engine, Hyper-V, libjpeg image-processing library, Adobe Type Manager Font Driver, Win32K, Microsoft Outlook, Internet Explorer, Graphics Component, Windows kernel-mode drivers and Lightweight Directory Access Protocol. This update also enables detection of processor generation and hardware support status when PC tries to scan or download updates through Windows Update.	KB4015546	**1**
04-2017 .NET Framework Security Update	This update resolves a vulnerability in the Microsoft .NET Framework that could allow remote code execution when the .NET Framework fails to properly validate input before loading libraries. An attacker who successfully exploits this vulnerability could take control of an affected system. The 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 learn more about this vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2017-0160.	KB4014573	**1**
03-2017 Security Only Multiple Update	This security update resolves the following vulnerabilities in Windows 7 SP1 and Windows Server 2008 R2 SP1: • MS17-022 Security update for Microsoft XML Core Services • MS17-021 Security update for DirectShow • MS17-020 Security update for Windows DVD Maker • MS17-019 Security update for Active Directory Federation Services • MS17-018 Security update for Windows Kernel-Mode Drivers • MS17-017 Security update for Windows Kernel • MS17-016 Security update for Internet Information Services • MS17-013 Security update for Microsoft Graphics Component • MS17-012 Security update for Microsoft Windows • MS17-011 Security update for Microsoft Uniscribe	KB4012212	**1**

	• MS17-010 Security update for Windows SMB Server • MS17-008 Security update for Windows Hyper-V		
04-2017 .NET Framework security update	This update resolves a vulnerability in the Microsoft .NET Framework that could allow remote code execution when the .NET Framework fails to properly validate input before loading libraries. An attacker who successfully exploits this vulnerability could take control of an affected system. The 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 learn more about this vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2017-0160.	KB4014558	**1**
03-2019 Cumulative Security Update for Internet Explorer	This security update resolves several reported vulnerabilities in Internet Explorer. The most severe of these vulnerabilities could allow remote code execution if a user views a specially crafted webpage in Internet Explorer. To learn more about these vulnerabilities, see Microsoft Common Vulnerabilities and Exposures.	KB4489873	**1**
03-2010 Security Update	This update helps protect against DLL preloading vulnerabilities in software applications on the Windows platform.	KB2264107	**1**

01-2019 Malicious Software Tool Update	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers that are running any of the following operating systems: • Windows 10 • Windows Server 2019 • Windows Server 2016 • Windows 8.1 • Windows Server 2012 R2 • Windows 8 • Windows Server 2012 • Windows 7 • Windows Server 2008	KB890830	**1**

The following are important updates for the BD EpiCenter on the Windows 7 operating system that were validated by BD:

Patch Name	Patch Description	Patch ID	Notes
02-2019 .NET 3.5.1 Framework Security update	This security update resolves vulnerabilities in Microsoft .NET Framework that could allow the following: • A Remote Code Execution vulnerability in .NET Framework software if the software does not check the source markup of a file. An attacker who successfully exploits the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on by using 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 that have full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who have administrative user rights.	KB4483483	**1**
02-2019 .NET 3.5.1 Quality rollup	This security update resolves vulnerabilities in Microsoft .NET Framework that could allow the following: • A Remote Code Execution vulnerability in .NET Framework software if the software does not check the source markup of a file. An attacker who successfully exploits the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on by using 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 that have full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who have administrative user rights.	KB4483458	

01-2019 Security rollup for Win7	This security update includes quality improvements. No new operating system features are being introduced in this update. Key changes include: • Provides protections against an additional subclass of speculative execution side-channel vulnerability known as Speculative Store Bypass (CVE-2018-3639) for AMD-based computers. These protections aren't enabled by default. For Windows client (IT pro) guidance, follow the instructions in KB4073119. For Windows Server guidance, follow the instructions in KB4072698. Use these guidance documents to enable mitigations for Speculative Store Bypass (CVE-2018-3639). Additionally, use the mitigations that have already been released for Spectre Variant 2 (CVE-2017-5715) and Meltdown (CVE-2017-5754). • Addresses an issue that affects PowerShell remoting loop back using non-administrator accounts. For more details, see Windows Security change affecting PowerShell. • Addresses an issue related to the date format for the Japanese Era calendar. For more information, see KB4469068. • Addresses an issue that causes the **GetCalendarInfo** function to return a wrong value for the Japanese Era. For more information, see KB4469068. • Security updates to Windows Kernel, Windows Storage and Filesystems, Windows Wireless Networking, and the Microsoft JET Database Engine.	KB4480960	
12-2018 Monthly Rollup for Win7	This security update includes quality improvements. No new operating system features are being introduced in this update. Key changes include: • Provides protections against an additional subclass of speculative execution side-channel vulnerability known as Speculative Store Bypass (CVE-2018-3639) for AMD-based computers. These protections aren't enabled by default. For Windows client (IT pro) guidance, follow the instructions in KB4073119. For Windows Server guidance, follow the instructions in KB4072698. Use these guidance documents to enable mitigations for Speculative Store Bypass (CVE-2018-3639). Additionally, use the mitigations that have already been released for Spectre Variant 2 (CVE-2017-5715) and Meltdown (CVE-2017-5754). • Addresses an issue that affects PowerShell remoting loop back using	KB4471328	**1**

	non-administrator accounts. For more details, see Windows Security change affecting PowerShell. • Addresses an issue related to the date format for the Japanese Era calendar. For more information, see KB4469068. • Addresses an issue that causes the **GetCalendarInfo** function to return a wrong value for the Japanese Era. For more information, see KB4469068. • Security updates to Windows Kernel, Windows Storage and Filesystems, Windows Wireless Networking, and the Microsoft JET Database Engine.		
12-2018 .NET 3.5.1 Framework Security	This security update resolves a vulnerability in Microsoft .NET Framework that could allow remote code execution when Microsoft .NET Framework doesn't validate input correctly. An attacker who successfully exploits this vulnerability could take control of an affected system. The attacker could then install programs; view, change, or delete data; or create new accounts that use full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.	KB4470600	**1**
08-2018 .NET 3.5.1 Framework Security	This security update resolves an information disclosure vulnerability in Microsoft .NET Framework that could allow an attacker to access information in multi-tenant environments. The vulnerability is caused when .NET Framework is used in high-load/high-density network connections in which content from one stream can blend into another stream.	KB4344177	**1**
07-2018 Security Update	This security update includes quality improvements. No new operating system features are being introduced in this update. Key changes include: • Provides protections for an additional vulnerability involving side-channel speculative execution known as Lazy Floating Point (FP) State Restore (CVE-2018-3665) for 64-Bit (x64) versions of Windows. • Security updates to Windows apps, Windows graphics, Windows Shell, Windows datacenter networking, Windows wireless networking, and Windows virtualization.	KB4338823	**1**

07-2018 .NET 3.5.1 Framework Security	This security update resolves the following vulnerabilities: • A "remote code execution" vulnerability exists when .NET Framework does not validate input correctly. An attacker who successfully exploits this vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts that have full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who have administrative user rights. To exploit the vulnerability, an attacker would have to pass specific input to an application through susceptible .NET Framework methods. This security update addresses the vulnerability by correcting how .NET Framework validates input. To learn more about this vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2018-8284. • An "elevation of privilege" vulnerability exists in .NET Framework that could allow an attacker to elevate their user rights level. To exploit the vulnerability, an attacker would first have to access the local computer, and then run a malicious program. This update addresses the vulnerability by correcting how .NET Framework enables COM objects. To learn more about this vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2018-8202. • A "security feature bypass" vulnerability exists when .NET Framework components do not correctly validate certificates. An attacker could present expired certificates when challenged. This security update addresses the vulnerability by making sure that .NET Framework components correctly validate certificates. To learn more about this vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2018-8356.	KB4338612	**1**
05-2018 Security Update	This update resolves a vulnerability in Microsoft .NET Framework that could cause denial of service when .NET Framework and .NET core components process XML documents incorrectly. An attacker who has successfully exploited this vulnerability could cause a denial of service against a .NET Framework application. To learn more about this vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2018-0765. Additionally, this update resolves a security feature bypass vulnerability in Windows that	KB4095514	**1**

	could allow an attacker to bypass Device Guard. An attacker who successfully exploits this vulnerability could circumvent a User Mode Code Integrity (UMCI) policy on the computer. To learn more about this vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2018-1039.		
12-2017 Security Update	This security update includes quality improvements. No new operating system features are being introduced in this update. Key changes include: • Addresses additional issues with updated time zone information. • Security updates to the Microsoft Scripting Engine and Windows Server.	KB4054521	**1**
11-2017 Security Update	This security update includes quality improvements. No new operating system features are being introduced in this update. Key changes include: • Addressed issue where applications based on the Microsoft JET Database Engine (Microsoft Access 2007 and older or non-Microsoft applications) fail when creating or opening Microsoft Excel .xls files. The error message is: "Unexpected error from external database driver (1). (Microsoft JET Database Engine)". • Security updates to Microsoft Windows Search Component, Windows Media Player, Microsoft Graphics Component, Windows kernel, and Windows kernel-mode drivers.	KB4048960	**1**
11-2017 .NET 3.5.1 Framework Security	This security update resolves a vulnerability in the Microsoft .NET Framework that could allow remote code execution when Microsoft .NET Framework processes untrusted input. An attacker who successfully exploits this vulnerability by using the .NET Framework could take control of an affected system. The attacker could then install programs; view, change, or delete data; or create new accounts that have full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate by using administrative user rights.	KB4040980	**1**

09-2017 .NET 3.5.1 Framework Security	This security update resolves a vulnerability in the Microsoft .NET Framework that could allow remote code execution when Microsoft .NET Framework processes untrusted input. An attacker who successfully exploits this vulnerability in software by using the .NET Framework could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts that have full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate by using administrative user rights.	KB4040966	**1**
10-2017 Security Update	This article describes an update that addresses an issue in Windows Server 2012, Windows 7 Service Pack 1 (SP1), and Windows Server 2008 R2 SP1 that is described in the following Knowledge Base article: The .NET Framework 4.7 installation is blocked on Windows 7, Windows Server 2008 R2 and Windows Server 2012 because of a missing d3dcompiler update	KB4019990	**1**
05-2017 .NET 3.5.1 Framework Security	This security update for the Microsoft .NET Framework resolves a security feature bypass vulnerability in which the .NET Framework (and the .NET Core) components do not completely validate certificates. To learn more about this vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2017-0248. This update also contains security-enhancing fixes to the Windows Presentation Framework **PackageDigitalSignatureManager** component's ability to sign packages with the SHA256 hash algorithm.	KB4014579	**1**
06-2016 MS16-077 WPAD Security Update	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if the Web Proxy Auto Discovery (WPAD) protocol falls back to a vulnerable proxy discovery process on a target system.	KB3161949	**1**
06-2016 MS16-072 Security Update	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker launches a man-in-the-middle (MiTM) attack against the traffic passing between a domain controller and the target machine.	KB3159398	**1**

05-2016 Security Update	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if Windows Media Center opens a specially crafted Media Center link (.mcl) file that references malicious code. An attacker who successfully exploited this vulnerability could gain the same user rights as the current user. Users whose accounts are configured to have fewer user rights on the system could be less affected than those who operate with administrative user rights.	KB3150220	**1**
03-2016 Security Update	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if the Windows Secondary Logon Service fails to properly manage request handles in memory.	KB3139914	**1**
03-2016 Security Update	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker with physical access inserts a specially crafted USB device into the system.	KB3139398	**1**
02-2016 MS16-019 .NET 3.5.1 Framework Security Update	This update resolves a vulnerability in the Microsoft .NET Framework. The vulnerability could allow denial of service if an attacker inserts specially crafted XSLT into a client-side XML web part that causes recursive calls on the server. To learn more about this vulnerability, see Microsoft Security Bulletin MS16-019.	KB3127220	**1**
02-2016 MS16-014 Security Only Multiple Update	This security update resolves vulnerabilities in Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application. To learn more about the vulnerabilities, see Microsoft Security Bulletin MS16-014.	KB3126587	**1**

02-2016 MS16-019 .NET 3.5.1 Framework security update	This update resolves a vulnerability in the Microsoft .NET Framework. The vulnerability could allow denial of service if an attacker inserts specially crafted XSLT into a client-side XML web part that causes recursive calls on the server. To learn more about this vulnerability, see Microsoft Security Bulletin MS16-019.	KB3122648	**1**
01-2016 MS16-007 Security Update	This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.	KB3121461	**1**
01-2016 MS16-007 Security Update	This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.	KB3110329	**1**
01-2016 MS16-007 Security Update	This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.	KB3109560	**1**
12-2015 MS15-133 Security Update	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to a targeted system and runs a specially crafted application that, by way of a race condition, results in references to memory locations that have already been freed. To learn more about the vulnerability, see Microsoft Security Bulletin MS15-133.	KB3109103	**1**

12-2015 Security Update	This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application. To learn more about the vulnerability, see Microsoft Security Bulletin MS16-007.	KB3108664	**1**
12-2015 MS15-132 Security Update	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if an attacker accesses a local system and runs a specially crafted application. To learn more about the vulnerability, see Microsoft Security Bulletin MS15-132.	KB3108371	**1**
10-2015 MS15-117 Security Update	This security update resolves a vulnerability in Microsoft Windows NDIS. The vulnerability could allow elevation of privilege if an attacker logs on to a system and runs a specially crafted application. To learn more about the vulnerability, see Microsoft Security Bulletin MS15-117.	KB3101722	**1**
10-2015 MS15-118 .NET Framework Security Update	This update resolves vulnerabilities in the Microsoft .NET Framework. The most severe of these vulnerabilities could allow elevation of privilege if an attacker injects a client-side script into a user's browser. To learn more about this vulnerability, see Microsoft Security Bulletin MS15-118.	KB3097989	**1**
11-2015 MS15-119 Security Update	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to a computer and runs specially crafted code that exploits the vulnerability. To learn more about the vulnerability, see Microsoft Security Bulletin MS15-119.	KB3092601	**1**

08-2015 MS15-082 Security Update	This security update resolves vulnerabilities in Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker first places a specially crafted dynamic link library (DLL) file in the target user's current working directory and then convinces the user to open an RDP file or to launch a program that is designed to load a trusted DLL file but instead loads the attacker's specially crafted DLL file. An attacker who successfully exploited the vulnerabilities could take complete control of an affected system. An attacker could then install programs, could view, change, or delete data, or could create new accounts that have full user rights. This security update addresses the vulnerability by correcting how the Remote Desktop Session Host (RDSH) validates certificates and how RDP loads certain binaries.	KB3075226	**1**
09-2015 MS15-101 Security Update	This update resolves vulnerabilities in the Microsoft .NET Framework that could allow elevation of privilege if a user runs a specially crafted .NET Framework application. To learn more about this vulnerability, see Microsoft Security Bulletin MS15-101.	KB3074543	**1**
08-2015 MS15-085 Security Update for Mount Manager	This security update resolves a vulnerability in Windows that could allow elevation of privilege if an attacker inserts a malicious USB device into a target system. An attacker could then write a malicious binary to disk and execute the code. To learn more about the vulnerability, see Microsoft Security Bulletin MS15-085.	KB3071756	**1**
07-2015 MS15-069 Security Update	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if an attacker first places a specially crafted dynamic link library (DLL) file in the target user's current working directory. Then, the attacker convinces the user to open an .rtf file or to start a program that is designed to load a trusted DLL file. But instead, the program loads the attacker's specially crafted DLL file. An attacker who successfully exploited the vulnerabilities could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts that have full user rights. To learn more about the vulnerability, see Microsoft Security Bulletin MS15-069.	KB3067903	**1**

08-2015 MS15-090 Security Update	To learn more about the vulnerability, see Microsoft Security Bulletin MS15-090.	KB3060716	**1**
06-2015 MS15-060 Security Update	This security update resolves a vulnerability in Windows that could allow remote code execution if a user clicks a specially crafted link or a link to specially crafted content and then invokes F12 developer tools in Internet Explorer.	KB3059317	**1**
05-2015 MS15-050 Security Update	This security update resolves a vulnerability in Windows Service Control Manager (SCM). This vulnerability is caused when SCM incorrectly verifies impersonation levels. The vulnerability could allow elevation of privilege if an attacker can first log on to the system and then run a specially crafted application that is designed to increase privileges.	KB3055642	**1**
04-2015 MS15-037 Security Update	This security update resolves a vulnerability in Microsoft Windows. An attacker who successfully exploited the vulnerability could take advantage of a known invalid task to cause Task Scheduler to run a specially crafted application in the context of the System account. An attacker could then do the following: • Install programs • View, change, or delete data • Create new accounts that have full user rights	KB3046269	**1**
08-2015 MS15-088 Security Update	This security update helps resolve an information disclosure vulnerability in Windows, Internet Explorer, and Microsoft Office. To exploit the vulnerability, an attacker would first have to use another vulnerability in Internet Explorer to run code in the sandboxed process. The attacker could then run Notepad, Visio, PowerPoint, Excel, or Word by using an unsafe command-line parameter to effect information disclosure. To be protected from the vulnerability, customers must apply the updates that are provided in this bulletin and also the update for Internet Explorer that is provided in MS15-079. Similarly,	KB3046017	**1**

	customers who are running an affected Office product must also install the applicable updates that are provided in MS15-081.		
04-2015 MS15-038 Security Update	This security update resolves vulnerabilities in Windows. These vulnerabilities could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application. To exploit the vulnerabilities, an attacker would first have to log on to the system. This security update addresses the vulnerabilities by correcting how Windows validates impersonation events. To learn more about the vulnerabilities, see Microsoft Security Bulletin MS15-038.	KB3045685	**1**
04-2015 MS15-041 .NET 3.5.1 Framework Security Update	This update resolves a vulnerability in the Microsoft .NET Framework that could allow information disclosure if an attacker sends a specially crafted web request to an affected server that has custom error messages disabled. An attacker who successfully exploits the vulnerability could view parts of a web configuration file that could expose sensitive information. To learn more about this vulnerability, see Microsoft Security Bulletin MS15-041. Note To resolve the vulnerability, you may have to apply multiple updates, depending on the versions of .NET Framework that you are running. For more information, see Versions of the .NET Framework that are affected by this security bulletin.	KB3037574	**1**
05-2015 MS15-048 .NET 3.5.1 Framework Security Update	Microsoft has released security bulletin MS15-048. Learn more about how to obtain the fixes that are included in this security bulletin: • For individual, small business, and organizational users, use the Windows automatic updating feature to install the fixes from Microsoft Update. To do this, see Get security updates automatically on the Microsoft Safety and Security Center website. • For IT professionals, see Microsoft Security Bulletin MS15-048 on the Security TechCenter website.	KB3023215	**1**

05-2017 .NET 4.5.2 Framework Security Update	This security update for the Microsoft .NET Framework resolves a security feature bypass vulnerability in which the .NET Framework (and the .NET Core) components do not completely validate certificates. To learn more about this vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2017-0248. This update also contains security-enhancing fixes to the Windows Presentation Framework **PackageDigitalSignatureManager** component's ability to sign packages with the SHA256 hash algorithm.	KB4014599	**1**
09-2017 .NET 4.5.2 Framework Security Update	This security update resolves a vulnerability in the Microsoft .NET Framework that could allow remote code execution when Microsoft .NET Framework processes untrusted input. An attacker who successfully exploits this vulnerability in software by using the .NET Framework could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts that have full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate by using administrative user rights.	KB4040960	**1**
11-2017 .NET 4.5.2 Framework Security Update	This security update resolves a vulnerability in the Microsoft .NET Framework that could allow remote code execution when Microsoft .NET Framework processes untrusted input. An attacker who successfully exploits this vulnerability by using the .NET Framework could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts that have full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate by using administrative user rights.	KB4040977	**1**
05-2018 .NET 4.5.2 Framework Security Update	This update resolves a vulnerability in Microsoft .NET Framework that could cause denial of service when .NET Framework and .NET core components process XML documents incorrectly. An attacker who has successfully exploited this vulnerability could cause a denial of service against a .NET Framework application. To learn more about this vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2018-0765. Additionally, this update resolves a security feature bypass vulnerability in Windows that could allow an attacker to bypass Device Guard. An attacker who successfully exploits this vulnerability could circumvent a User Mode Code Integrity (UMCI) policy on the computer. To learn more about this vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2018-1039.	KB4095519	**1**

08-2018 .NET 4.5.2 Framework Security Update	This security update resolves the following vulnerabilities: • A "remote code execution" vulnerability exists when .NET Framework does not validate input correctly. An attacker who successfully exploits this vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts that have full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who have administrative user rights. To exploit the vulnerability, an attacker would have to pass specific input to an application through susceptible .NET Framework methods. This security update addresses the vulnerability by correcting how .NET Framework validates input. To learn more about this vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2018-8284. • An "elevation of privilege" vulnerability exists in .NET Framework that could allow an attacker to elevate their user rights level. To exploit the vulnerability, an attacker would first have to access the local computer, and then run a malicious program. This update addresses the vulnerability by correcting how .NET Framework enables COM objects. To learn more about this vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2018-8202. • A "security feature bypass" vulnerability exists when .NET Framework components do not correctly validate certificates. An attacker could present expired certificates when challenged. This security update addresses the vulnerability by making sure that .NET Framework components correctly validate certificates. To learn more about this vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2018-8356.	KB4338602	**1**
08-2018 .NET 4.5.2 Framework Security Update	This security update resolves an information disclosure vulnerability in Microsoft .NET Framework that could allow an attacker to access information in multi-tenant environments. The vulnerability is caused when .NET Framework is used in high-load/high-density network connections in which content from one stream can blend into another stream.	KB4344173	**1**

12-2018 .NET 4.5.2 Framework Security Update	This security update resolves a vulnerability in Microsoft .NET Framework that could allow remote code execution when Microsoft .NET Framework doesn't validate input correctly. An attacker who successfully exploits this vulnerability could take control of an affected system. The attacker could then install programs; view, change, or delete data; or create new accounts that use full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.	KB4470493	**1**
02-2019 .NET 4.5.2 Framework Security Update	This security update resolves vulnerabilities in Microsoft .NET Framework that could allow the following: • A Remote Code Execution vulnerability in .NET Framework software if the software does not check the source markup of a file. An attacker who successfully exploits the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on by using 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 that have full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who have administrative user rights.	KB4483455	**1**
02-2019 .NET 4.5.2 Framework Security Update	This security update resolves vulnerabilities in Microsoft .NET Framework that could allow the following: • A Remote Code Execution vulnerability in .NET Framework software if the software does not check the source markup of a file. An attacker who successfully exploits the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on by using 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 that have full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who have administrative user rights.	KB4483474	**1**

Notes

1. Tested against BD EpiCenter configured with Windows 7 Professional 64-bit.