BD EpiCenter™

Date of Critical or Security Patches: April 2021

Critical Security Patches: February 2015 - October 2020

Microsoft® & Third-Party Patches for Windows 7

BD has identified patches from Microsoft® that have been identified as critical or important security related updates thru October 2020. 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
Security Update for Windows 7	This security update resolves a privately reported vulnerability in Microsoft Windows. A remote code execution vulnerability exists in how Group Policy receives and applies connection data when a domain-joined system connects to a domain controller	KB3000483	
.NET 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.	KB4014591	
.NET 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.	KB4014579	
.NET 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	KB4014558	
Update for D3DCompiler_47.dll	The .NET Framework 4.7 installation is blocked on Windows7 because of a missing d3dcompiler update.	KB4019990	
.NET 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.	KB4040957	
.NET 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.	KB4040966	
.NET Security Update	This security update resolves a vulnerability in the Microsoft .NET	KB4040973	

	Framework that could allow remote code execution when Microsoft .NET Framework processes untrusted input.		
.NET 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.	KB4040980	
.NET 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.	KB4095514	
.NET 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.	KB4096237	
.NET Security Update	▪ 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	KB4338606	

	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.		
.NET Security Update	▪ 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	KB4338612	

	that .NET Framework components correctly validate certificates. To learn more about this vulnerability, see Microsoft Common Vulnerabilities and Exposures CVE-2018-8356.		
.NET 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.	KB4344167	
.NET 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.	KB4344177	
Security Update for Windows 7	This update introduces SHA-2 code sign support for Windows 7 SP1, Windows Server 2008 R2 SP1, and Windows Server 2008 SP2.	KB4474419	
Servicing Stack Update	This update makes quality improvements to the servicing stack component that installs Windows updates.	KB4490628	
.NET Security Update	Denial of service vulnerabilities exist when .NET Framework improperly handles objects in heap memory, or when .NET Framework and .NET Core improperly process RegEx strings.	KB4495587	
.NET Security Update	Denial of service vulnerabilities exist when .NET Framework improperly handles objects in heap memory, or when .NET Framework and .NET Core improperly process RegEx strings.	KB4495612	
.NET Security Update	A remote code execution vulnerability exists in .NET software when the software fails to check the source markup of a file. An Authentication Bypass vulnerability exists in WCF and WIF, allowing signing of SAML tokens with arbitrary symmetric keys.	KB4506963	
.NET Security Update	A remote code execution vulnerability exists in .NET software when the software fails to check the source markup of a file. An Authentication Bypass vulnerability exists in WCF and WIF, allowing signing of SAML tokens with arbitrary symmetric keys.	KB4506976	
Servicing Stack Update	This update makes quality improvements to the servicing stack component that installs Windows updates.	KB4516655	
Security Update for Windows 7	▪ Updates time zone information for Norfolk Island, Australia.	KB4519972	

	▪ Updates time zone information for the Fiji Islands. ▪ Addresses an issue with evaluating the compatibility status of the Windows ecosystem to help ensure application and device compatibility for all updates to Windows. For more information, see KB4525208. ▪ Addresses an issue that prevents **netdom.exe** from displaying the new ticket-granting ticket (TGT) delegation bit for the display or query mode.		
Servicing Stack Update	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates.	KB4531786	
.NET Security Update	A remote code execution vulnerability exists when the Microsoft .NET Framework fails to validate input properly.	KB4532960	
.NET Security Update	A remote code execution vulnerability exists when the Microsoft .NET Framework fails to validate input properly.	KB4532971	
.NET Security Update	An elevation of privilege vulnerability exists in .NET Framework which could allow an attacker to elevate their privilege level. The update addresses the vulnerability by correcting how .NET Framework activates COM objects.	KB4552965	
Security Update for Internet Explorer	This security update resolves vulnerabilities in Internet Explorer	KB4556798	
Security Update for Windows 7	▪ Updates the 2020 start date for daylight saving time (DST) in the Kingdom of Morocco. For more information, see KB4557900. ▪ Security updates to Windows App Platform and Frameworks, Windows Apps, Windows Input and Composition, Windows Kernel, Internet Information Services, Windows Network Security and Containers, Windows Active Directory, the Microsoft JET Database Engine, and Windows Storage and Filesystems.	KB4556843	
Servicing Stack Update for Windows 7	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates.	KB4570673	
Security Update for Windows 7	This security update includes quality improvements. Key changes include:	KB4571719	

	▪ Security updates to Windows App Platform and Frameworks, Windows Graphics, Windows Media, Windows Cloud Infrastructure, Windows Authentication, Windows Kernel, Windows Hybrid Cloud Networking, Windows Peripherals, Windows Storage and Filesystems, Windows Network Security and Containers, Windows File Server and Clustering, Windows Hybrid Storage Services, Microsoft Scripting Engine, and Windows SQL components.		
Update for Windows 7 Extended Security Updates License	This update provides an additional set of licensing changes to enable installation of the ESU add-on key.	KB4575903	
Security Update for Windows 7	▪ Addresses an issue that might cause the Graphics Device Interface (GDI) to access internal regions incorrectly causing unexpected UI experiences. This issue can cause additional or missing screen elements, screen flickering, or a trailing screen. ▪ Corrects the end date for daylight savings time (DST) in 2021 for the Fiji Islands. For more information, see DST correction in Windows for the Fiji Islands: October 13, 2020. ▪ Addresses an issue where Group Policy recursively deletes critical files when the "Delete local user profile policy" is enabled. ▪ Addresses an issue in which a Null port is created through the user interface. ▪ Security updates to Windows App Platform and Frameworks, Windows Graphics, Windows Shell, Windows Silicon Platform, Windows Cloud Infrastructure, Windows Fundamentals, Windows Authentication, Windows Virtualization, Windows Core Networking, Windows Network Security and Containers, Windows Storage and Filesystems, Windows SQL components, and Windows Remote Desktop.	KB4580345	

Notes

Advancing the world of health