BD Product Name: **Identity provider management (IDM)**

Date of Critical or Security Patches: March 2021
Abstract: Critical or Security Patches – March 2021

Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for March 2021. 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	Description	Patch ID	Notes
2021-03 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems (KB5000800)	• As of February 11, 2020, Internet Explorer 10 is no longer in support. To get Internet Explorer 11 for Windows Server 2012 or Windows 8 Embedded Standard, see KB4492872. Install one of the following applicable updates to stay updated with the latest security fixes: ○ Cumulative Update for Internet Explorer 11 for Windows Server 2012. ○ Cumulative Update for Internet Explorer 11 for Windows 8 Embedded Standard. ○ The March 2021 Monthly Rollup. • Some customers using Windows Server 2008 R2 SP1 who activated	KB5000800	N/A

	their ESU multiple activation key (MAK) add-on before installing the January 14, 2020 updates might need to re-activate their key. Re-activation on affected devices should only be required once. For information on activation, see this blog post. WSUS scan cab files will continue to be available for Windows 7 SP1 and Windows Server 2008 R2 SP1. If you have a subset of devices running these operating systems without ESU, they might show as non-compliant in your patch management and compliance toolsets.		
Windows Malicious Software Removal Tool x64 - v5.85	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 Server 2012 Windows 7 Windows Server 2008 R2 for x64-based Systems	KB890830	N/A
2021-03 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5000848)	This security update includes improvements and fixes that were a part of update KB4601384 (released February 9, 2021) and addresses the following issues:	KB5000848	N/A

	• Addresses an issue in which a non-native device that is in the same realm does not receive a Kerberos Service ticket from Active Directory DCs. This issue occurs even though Windows Updates are installed that contain CVE-2020-17049 protections released between November 10 and December 8, 2020 and configured **PerfromTicketSignature** to **1** or larger. Ticket acquisition fails with **KRB_GENERIC_ERROR** if callers submit a PAC-less Ticket Granting Ticket (TGT) as an evidence ticket without the **USER_NO_AUTH_DATA_REQUIRED** flag being set for the user in User Account Controls. • Addresses an elevation of privilege security vulnerability documented in CVE-2021-1640 related to print jobs submitted to "FILE:" ports. After installing Windows updates from March 9, 2021 and later, print jobs that are in a pending state before restarting the print spooler service or restarting the OS will remain in an error state. Manually delete the affected print jobs and resubmit them to		

	the print queue when the print spooler service is online. • Security updates to Windows Fundamentals, Windows Shell, Windows UAC, Windows Hybrid Cloud Networking, Windows Media, and Windows Graphics.		
2021-03 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5000853)	This security update includes quality improvements. Key changes include: • Addresses an issue in which a non-native device that is in the same realm does not receive a Kerberos Service ticket from Active Directory DCs. This issue occurs even though Windows Updates are installed that contain CVE-2020-17049 protections released between November 10 and December 8, 2020 and configured **PerfromTicketSignature** to **1** or larger. Ticket acquisition fails with **KRB_GENERIC_ERROR** if callers submit a PAC-less Ticket Granting Ticket (TGT) as an evidence ticket without the **USER_NO_AUTH_DATA_REQUIRED** flag being set for the user in User Account Controls.	KB5000853	N/A

	• Security updates to Windows Fundamentals, Windows Shell, Windows UAC, Windows Hybrid Cloud Networking, Windows Media, and Windows Graphics.		
2021-03 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5000803)	This security update includes quality improvements. Key changes include: • Turns off token binding by default in Windows Internet (WinINet). • Addresses an issue in the Windows Management Instrumentation (WMI) service that causes a heap leak each time security settings are applied to WMI namespace permissions. • Addresses an issue in which a principal in a trusted MIT realm fails to obtain a Kerberos service ticket from Active Directory domain controllers (DC). This occurs on devices that installed Windows Updates that contain CVE-2020-17049 protections and configured PerfromTicketSignature to 1 or higher. These updates were released between November 10, 2020 and December 8, 2020. Ticket acquisition also fails with the error,	KB5000803	N/A

	“KRB_GENERIC_ERROR”, if callers submit a PAC-less Ticket Granting Ticket (TGT) as an evidence ticket without providing the USER_NO_AUTH_DATA_REQUIRED flag. - Addresses an elevation of privilege security vulnerability documented in CVE-2021-1640 related to print jobs submitted to “FILE:” ports. After installing Windows updates from March 9, 2021 and later, print jobs that are in a pending state before restarting the print spooler service or restarting the OS will remain in an error state. Manually delete the affected print jobs and resubmit them to the print queue when the print spooler service is online. - Addresses a reliability issue in Remote Desktop. - Addresses an issue that might cause stop error 7E in **nfssvr.sys** on servers running the Network File System (NFS) service. - Adds a new dfslogkey as described below: Keypath: **HKEY_LOCAL_MACHINE/SOFTWARE/MICROSOFT/dfslog**. The RootShareAcquireSuccessEve		

	nt field has the following possible values: Default value = 1; enables the log. Value other than 1; disables the log. If this key does not exist, it will be created automatically. To take effect, any change to dfslog/RootShareAcquireSuccessEvent in the registry requires that you restart the DFSN service. • Addresses an issue that causes an increase in network traffic during update detection for Windows Updates. This issue occurs on devices that are configured to use an authenticated user proxy as the fallback method if update detection with a system proxy fails or there is no proxy. • Security updates to the Windows Shell, Windows User Account Control (UAC), Windows Fundamentals, Windows Core Networking, Windows Hybrid Cloud Networking, Windows Kernel, Windows Virtualization, the Microsoft Graphics Component, Internet Explorer, Microsoft		

	Edge Legacy, and Windows Media.		
2021-01 Update for Windows Server 2016 for x64-based Systems (KB4589210)	This update for some select products (CPUs) is available through Windows Update. It will be downloaded and installed automatically. For more information	KB4589210	N/A