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

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

Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for July 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
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
2021-07 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5004298)	This security update includes improvements and fixes that were a part of update KB5004954 (released July 6, 2021) and addresses the following issues: Addresses an issue in which 16-bit applications fail with an error message that states a general fault in VBRUN300.DLL. Addresses an issue in which some EMFs built by using	KB5004298	N/A

	third-party applications that use **ExtCreatePen** and **ExtCreateFontIndirect** render incorrectly. Adds Advanced Encryption Standard (AES) encryption protections for CVE-2021-33757. For more information, see KB5004605.		
2020-12 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB4592495)	This security update includes quality improvements. Key changes include: Security updates to Windows Graphics, Windows Peripherals, and Windows Core Networking.	KB4592495	N/A
2021-07 Security and Quality Rollup for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 for x64 (KB5004231)	4578953 Description of the Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 (KB4578953) 4578956 Description of the Security and Quality Rollup for .NET Framework 4.5.2 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 (KB4578956) 5004122 Description of the Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 (KB5004122) 5004118 Description of the Security and Quality Rollup for .NET Framework 4.8 for	KB5004231	N/A

	Windows 8.1, RT 8.1, and Windows Server 2012 R2 (KB5004118)		
Security Update for Microsoft ASP.NET MVC 3 (KB2993937)	This update will be offered through Microsoft Update, the Microsoft Download Center, and updated NuGet packages. The security bulletin will provide correct guidance about which deployment option is required to help make sure that your computer and applications are secure.	KB2993937	N/A
2021-07 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5004238)	Removes support for the PerformTicketSignature setting and permanently enables Enforcement mode for CVE-2020-17049. For more information and steps to enable full protection on domain controller servers, see Managing deployment of Kerberos S4U changes for CVE-2020-17049. Addresses an issue that incorrectly renders some Enhanced Metafile Format (EMF) files. This issue occurs if you build the EMF files using third-party applications with **ExtCreatePen()** and **ExtCreateFontIndirect()**. Addresses a redirector stop error that is caused by a race condition that occurs when the system deletes binding objects when connections close. Removes the Adobe Flash component from your device. Adds Advanced Encryption Standard (AES) encryption	KB5004238	N/A

	protections for CVE-2021-33757. For more information, see KB5004605. Addresses a vulnerability in which Primary Refresh Tokens are not strongly encrypted. This issue might allow the tokens to be reused until the token expires or is renewed. For more information about this issue, see CVE-2021-33779. Security updates to Windows Apps, Windows Fundamentals, Windows Authentication, Windows User Account Control (UAC), Operating System Security, the Windows Kernel, Windows Graphics, the Microsoft Scripting Engine, the Windows HTML Platforms, the Windows MSHTML Platform, and Windows Active Directory.		
2021-07 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5004948)	Addresses a remote code execution exploit in the Windows Print Spooler service, known as "PrintNightmare", as documented in CVE-2021-34527. After installing this and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system's Trusted Root Certification Authorities trusts signed drivers. Microsoft recommends that you	KB5004948	N/A

	immediately install this update on all supported Windows client and server operating system, starting with devices that currently host the print server role. You also have the option to configure the **RestrictDriverInstallationToAdministrators** registry setting to prevent non-administrators from installing signed printer drivers on a print server. For more information, see KB5005010.		