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

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

Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for February 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
2021-02 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB4601384)	This security update includes improvements and fixes that were a part of update KB4598285 (released January 12, 2021) and addresses the following issues: • Addresses historical daylight saving time (DST) updates and corrections for the Palestinian Authority. • Addresses an issue with German translations of Central European Time. • Updates the Netlogon Elevation of Privilege Vulnerability (CVE-2020-1472) to enable Enforcement mode. For more details, see CVE-2020-1472 and How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472.	KB4601384	None

	• Security updates to Windows App Platform and Frameworks, Windows Hybrid Cloud Networking, and Windows Core Networking.		
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	None
2021-02 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 (KB4603004)	This security update addresses a denial of service vulnerability in .NET Framework.	KB4603004	None
2021-02 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB4601349)	Adds historical daylight saving time (DST) updates and corrections for the Palestinian Authority. Addresses an issue with German translations of Central European Time. Updates the Netlogon Elevation of Privilege Vulnerability (CVE-2020-1472) to enable Enforcement mode. For more details, see CVE-2020-1472 and How to manage the changes in Netlogon secure channel	KB4601349	None

	connections associated with CVE-2020-1472. Security updates to Windows App Platform and Frameworks, Windows Hybrid Cloud Networking, and Windows Core Networking.		
2021-02 Security Only Update for .NET Framework 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 (KB4602960)	This security update addresses a denial of service vulnerability in .NET Framework.	KB4602960	None
SQL Server 2016 Service Pack 2 Cumulative Update (CU) 16 KB5000645	This article describes Cumulative Update package 16 (CU16) (build number: **13.0.5882.1**) for Microsoft SQL Server 2016 Service Pack 2 (SP2). This update contains fixes that were released after the initial release of SQL Server 2016 SP2.	KB5000645	None
2021-02 Servicing Stack Update for Windows Server 2016 for x64-based Systems (KB5001078)	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.	KB5001078	None
2021-02 Cumulative Update for Windows Server 2016 for x64-based Systems (KB4601318)	Enables administrators to disable standalone Internet Explorer using a Group Policy while continuing to use Microsoft Edge's IE Mode.	KB4601318	None

	Updates Internet Explorer's About dialog to use the standard modern dialog. Addresses an issue with a Service Host (**svchost.exe**) process that causes excessive CPU usage in some Input Method Editor (IME) language environments, such as Traditional Chinese. This issue occurs when you try to add an input method in Control Panel. Corrects historical daylight savings time (DST) information for the Palestinian Authority. Addresses an issue with German translations of Central European Time. Addresses an issue that causes **LSASS.exe** to stop working because of a race condition that results in a double free error in Schannel. The exception code is c0000374, and the Event Log displays Schannel event 36888, fatal error code 20, and error state 960. This issue occurs after installing Windows updates from September 2020 and later. Addresses an issue that might cause systems that use BitLocker to stop working and display the error 0x120 (BITLOCKER_FATAL_ERROR). Addresses an issue that prevents scheduled tasks that have multiple actions from running again if you have		

	previously disabled them while they were running. Addresses an issue that fails to log events 4732 and 4733 for Domain-Local group membership changes in certain scenarios. This occurs when you use the "Permissive Modify" control; for example, the Active Directory (AD) PowerShell modules use this control. Addresses an issue that incorrectly reports that Lightweight Directory Access Protocol (LDAP) sessions are unsecure in Event ID 2889. This occurs when the LDAP session is authenticated and sealed with a Simple Authentication and Security Layer (SASL) method. Addresses an issue with Server Message Block (SMB). This issue incorrectly logs the Microsoft-Windows-SMBClient 31013 event in the Microsoft-Windows-SMBClient or Security event log of an SMB client when an SMB server returns STATUS_USER_SESSION_DELETED. This issue occurs when SMB client users or applications open multiple SMB sessions using the same set of Transmission Control Protocol (TCP) connections on the same SMB Server. This issue most likely occurs on Remote Desktop Servers. Addresses an issue that causes the LanmanServer service to stop unexpectedly. This issue occurs if the		

	OptionalNames registry value is set and the service restarts. Addresses an issue that causes stop error 0x54 in **SRV2.SYS**. Updates the Netlogon Elevation of Privilege Vulnerability		