Security Patches: Identity Management

April 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for April 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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).

Microsoft® patches

Patch name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 – v5.99	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 Server 2008 R2 • Windows 7 • Windows Server 2008	KB890830	N/A

2022-04 Security Quality Monthly Rollup for Windows Server 2012 R2 for x64-based Systems	This security update includes improvements and fixes that were a part of update KB5011564 (released March 8, 2022) and addresses the following issues: • Addresses an issue in Windows Media Center where some users might have to reconfigure the application on each start. • Addresses a memory leak that was introduced by the **PacRequestorEnforcement** registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain controllers. • Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. • Addresses an issue in which Windows might go into BitLocker recovery after a servicing update. • Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames. • Addresses an issue that causes a Denial of Service vulnerability on Cluster Shared Volumes (CSV). For more information, see CVE-2020-26784. • Addresses an issue that prevents you from changing a password that has expired when you sign in to a Windows device.	KB5012670	N/A
2022-04 Security-only Quality Update for Windows Server 2012 R2 for x64-based Systems	This security update includes quality improvements: • Addresses an issue in Windows Media Center where some users might have to reconfigure the application on each start. • Addresses a memory leak that was introduced by the **PacRequestorEnforcement** registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain controllers. • Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. • Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames.	KB5012639	N/A

2022-04 Servicing stack update for Windows Server 2012 R2 for x64-based Systems	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. Additionally, this update address an issue in which Windows might go into **BitLocker recovery** after a servicing update.	KB5012672	N/A
2022-04 Servicing stack update for Windows Server 2012 R2 for x64-based Systems	This security update includes quality improvements. Key changes include: • Addresses a heap leak in **PacRequestorEnforcement** that degrades the performance of a domain controller. • Addresses an issue that affects the Key Distribution Center (KDC) Proxy. The KDC Proxy cannot properly obtain Kerberos tickets for signing in to Key Trust Windows Hello for Business. • Addresses an issue that logs Event ID 37 during certain password change scenarios, including failover cluster name object (CNO) or virtual computer object (VCO) password changes. • Addresses an issue that causes a Denial of Service vulnerability on Cluster Shared Volumes (CSV). For more information, see **CVE-2020-26784**. • Addresses an issue that prevents you from changing a password that has expired when you sign in to a Windows device.	KB5012596	N/A

2022-04 Update for Windows Server 2016 for x64-based Systems	This new release includes a microcode update from Intel for the numerous CPUs.	KB4589210	**N/A**
2022-04 Security Update for Windows Server 2016 for x64-based Systems	This security update makes improvements to Secure Boot DBX for the supported Windows versions listed in the "Applies to" section. Key changes include the following: • Windows devices that has Unified Extensible Firmware Interface (UEFI) based firmware can run with Secure Boot enabled. The Secure Boot Forbidden Signature Database (DBX) prevents UEFI modules from loading. This update adds modules to the DBX. A security feature bypass vulnerability exists in secure boot. An attacker who successfully exploited the vulnerability might bypass secure boot and load untrusted software. This security update addresses the vulnerability by adding the signatures of the known vulnerable UEFI modules to the DBX.	KB4535680	**N/A**