

# Security Patches: Identity Management

September 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for September 2023. 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
Remove specific prevalent malware with Windows Malicious Software Removal Tool (KB890830)	This update addresses an issue that affects remote procedure calls (RPC) to the Win32_User or Win32_Group WMI class. The domain member that runs the RPC contacts the primary domain controller (PDC). When multiple RPCs occur at the same time on many domain members, this might overwhelm the PDC.	<a href="#">KB890830</a>	N/A
Servicing stack update for Windows Server 2016: (KB5030504)	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.	<a href="#">KB5030504</a>	N/A
OS Build 14393.6252 (KB5030213)	Microsoft releases the MSRT on a monthly cadence as part of Windows Update or as a standalone tool. Use this tool to find and remove specific prevalent threats and reverse the changes they have made (see covered malware families). For comprehensive malware detection and removal, consider using Windows Defender Offline or Microsoft Safety Scanner.	<a href="#">KB5030213</a>	N/A

Cumulative security update for Internet Explorer (KB5030209)	The improvements that are included in this Internet Explorer update are also included in the September 2023 Monthly Rollup. Installing either this Internet Explorer update or the Monthly Rollup installs the same improvements.	<a href="#">KB5030209</a>	N/A
Security-only update (KB5030287)	The Lanman Server Service might crash in clusters that do not have an Administrative Access Point, also known as AD-Detached Clusters. Using AD-Detached Clusters is recommended by Exchange on some versions of Windows. For more information, see Database availability groups.	<a href="#">KB5030287</a>	N/A
Security Only Update for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 (KB5030175)	CVE-2023-36796 - .NET Framework Remote Code Execution Vulnerability. This security update addresses a vulnerability in DiaSymReader.dll when reading a corrupted PDB file which can lead to Remote Code Execution. For more information see CVE 2023-36796.	<a href="#">KB5030175</a>	N/A
Monthly Rollup (KB5030269)	Authentication to join or re-join a computer to an Active Directory domain might fail when a user uses a Smart Card. This issue might occur after you install Windows Updates dated on or after November 2022.	<a href="#">KB5030269</a>	N/A
Security and Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 (KB5030184)	CVE-2023-36792 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in DiaSymReader.dll when reading a corrupted PDB file which can lead to Remote Code Execution.	<a href="#">KB5030184</a>	N/A

Servicing stack update for  
Windows Server 2012 R2  
(KB5030329)

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.

[KB5030329](#)

N/A

BD, Franklin Lakes, NJ, 07417, U.S.  
201.847.6800

[bd.com](#)

BD and the BD Logo are trademarks of Becton, Dickinson and Company or its affiliates. © 2022 BD. All rights reserved.

