

Security Patches: Identity Management

March 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for March 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: <ul style="list-style-type: none">• 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

2022-03 Cumulative Update for Windows Server 2016 for x64-based Systems	<p>This security update includes quality improvements. Key changes include:</p> <ul style="list-style-type: none"> • Addresses an issue that prevents printing from operating properly for some low integrity process apps. • Addresses an issue that causes Windows to go into BitLocker recovery after a servicing update. 	KB5011495	N/A
2022-03 Servicing Stack Update for Windows Server 2016 for x64-based Systems	<p>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 addresses an issue in which Windows might go into BitLocker recovery after a servicing update.</p>	KB5011570	N/A
2022-03 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based Systems	<p>This security update resolves vulnerabilities in Internet Explorer. To learn more about these vulnerabilities, see the Security Update Guide website. Additionally, see the following articles for more information about cumulative updates:</p> <ul style="list-style-type: none"> ▪ Windows Server 2008 SP2 update history ▪ Windows 7 SP1 and Windows Server 2008 R2 SP1 update history ▪ Windows Server 2012 update history ▪ Windows 8.1 and Windows Server 2012 R2 update history 	KB5011486	N/A
2022-03 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems	<p>This security update includes quality improvements. Key changes include:</p> <ul style="list-style-type: none"> • Addresses an issue in which some low integrity level process apps might print unexpectedly. • Addresses an issue that occurs when you try to write a service principal name (SPN) alias (such as www/contoso) and HOST/NAME already exists on another object. If the user has the RIGHT_DS_WRITE_PROPERTY on the SPN attribute of the colliding object, you receive an "Access Denied" error. • Addresses an issue in which after the January 2022 Windows update is installed on the Primary Domain Controller emulator (PDCe), listing or modifying name suffixes routing by using Netdom.exe or "Active Directory Domains and Trusts" snap-in may fail with the following error message: "Insufficient system resources exist to complete the requested service." 	KB5011560	N/A



2022-03 Security Monthly
Quality Rollup for Windows
Server 2012 R2 for x64-
based Systems

This security update includes improvements and fixes that were a part of update KB5010419 (released February 8, 2022) and addresses the following issues:

- Addresses an issue in which some low integrity level process apps might print unexpectedly.
- Addresses an issue that occurs when you try to write a service principal name (SPN) alias (such as www/contoso) and HOST/NAME already exists on another object. If the user has the RIGHT_DS_WRITE_PROPERTY on the SPN attribute of the colliding object, you receive an "Access Denied" error.
- Addresses an issue in which after the January 2022 Windows update is installed on the Primary Domain Controller emulator (PDCe), listing or modifying name suffixes routing by using Netdom.exe or "Active Directory Domains and Trusts" snap-in may fail with the following error message: "Insufficient system resources exist to complete the requested service."

[KB5011564](#)

N/A

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

[bd.com](https://www.bd.com)

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

