Security Patches:
BD Pyxis™ Med Station ES

June 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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 - v5.102	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	Applicable on MedSTN device.
2022-06 Cumulative Update for Windows 10 Version 1809 for x64-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5014692	Applicable on MedSTN device.

2022-06 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems.	This cumulative security update contains improvements that are part of update KB5014012 (released May 10, 2022) and includes new improvements for the following issue: Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures.	KB5014748	Applicable on MedSTN device.
2022-06 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems.	This security-only update includes new improvements for the following issue: Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures.	KB5014742	Applicable on MedSTN device.
2022-06 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems	This cumulative security update includes improvements that are part of update KB5014011 (released May 10, 2022) and includes new improvements for the following issue: Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures. Addresses an elevation of privilege (EOP) vulnerability under CVE-2022-30154 for the Microsoft File Server Shadow Copy Agent Service. To become protected and functional, you must install the June 14, 2022 or later Windows update on both the application server and the file server. The application server runs the Volume Shadow Copy Service (VSS)-aware application that stores data on the remote Server Message Block 3.0 (or higher) shares on a file server. The file server hosts the file shares. If you don't install the update on both machine roles, backup operations carried out by applications, which previously worked, might fail. For such failure scenarios, the Microsoft File Server Shadow Copy Agent Service will log FileShareShadowCopyAgent event 1013 on the file server.	KB5014738	Applicable on MedSTN devices.

2022-06 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems	This security-only update includes new improvements for the following issue: Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures. Addresses an elevation of privilege (EOP) vulnerability under CVE-2022-30154 for the Microsoft File Server Shadow Copy Agent Service. To become protected and functional, you must install the June 14, 2022 or later Windows update on both the application server and the file server. The application server runs the Volume Shadow Copy Service (VSS)-aware application that stores data on the remote Server Message Block 3.0 (or higher) shares on a file server. The file server hosts the file shares. If you don't install the update on both machine roles, backup operations carried out by applications, which previously worked, might fail. For such failure scenarios, the Microsoft File Server Shadow Copy Agent Service will log FileShareShadowCopyAgent event 1013 on the file server.	KB5014746	Applicable on MedSTN devices.

2022-06 Cumulative Update for Windows Server 2016 for x64-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5014702	Applicable on MedSTN device.

2022-06 Cumulative Update for Windows 10 Version 1607 for x64-based Systems.	This security update includes quality improvements. Key changes include: Provides a Group Policy that administrators can use to enable customers to use the Ctrl+S (Save As) keyboard shortcut in Microsoft Edge IE Mode. Addresses an issue that prevents printing from operating properly for some low integrity process apps. Addresses an issue that causes print failures when a low integrity level (LowIL) application prints to a null port. Addresses an issue that prevents you from signing in to Citrix servers that have enabled the Interactive logon: Require smart card security policy setting. Addresses an issue that causes a mismatch between a Remote Desktop session's keyboard and the Remote Desktop Protocol (RDP) client when signing in. Addresses an issue that prevents the file system control code (FSCTL_SET_INTEGRITY_INFORMATION_EX) from handling its input parameter correctly. Addresses an elevation of privilege (EOP) vulnerability under CVE-2022-30154 for the Microsoft File Server Shadow Copy Agent Service. To become protected and functional, you must install the June 14, 2022 or later Windows update on both the application server and the file server. The application server runs the Volume Shadow Copy Service (VSS)-aware application that stores data on the remote Server Message Block 3.0 (or higher) shares on a file server. The file server hosts the file shares. If you don't install the update on both machine roles, backup operations carried out by applications, which previously worked, might fail.	KB5014702	Applicable onMedSTN device.

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.

Security Patches: BD Pyxis CIISafe

June 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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
2022-06 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5014702	Applicable to CIISafe device.
Windows Malicious Software Removal Tool x64 - v5.102	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	Applicable to CIISafe device.

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.

Security Patches: BD Pharmogistics

June 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for June 2022. These patches were not found to adversely affect BD Pharmogistics 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	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	Applicable on PLX, CII Safe and Infusion.

2022-06 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems	This cumulative security update includes improvements that are part of update KB5014011 (released May 10, 2022) and includes new improvements for the following issue: • Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures. • Addresses an elevation of privilege (EOP) vulnerability under CVE-2022-30154 for the Microsoft File Server Shadow Copy Agent Service.	KB5014738	Applicable on PLX, CII Safe and Infusion.
2022-06 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems	**This security-only update includes new improvements for the following issue:** • **Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures.** • **Addresses an elevation of privilege (EOP) vulnerability under CVE-2022-30154 for the Microsoft File Server Shadow Copy Agent Service.**	KB5014746	Applicable on PLX, CII Safe and Infusion.

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.

Security Patches: TIM

June 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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
2022-06 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems	This cumulative security update includes improvements that are part of update KB5014011 (released May 10, 2022) and includes new improvements for the following issue: Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures. Addresses an elevation of privilege (EOP) vulnerability under CVE-2022-30154 for the Microsoft File Server Shadow Copy Agent Service. To become protected and functional, you must install the June 14, 2022 or later Windows update on both the application server and the file server. The application server runs the Volume Shadow Copy Service (VSS)-aware application that stores data on the remote Server Message Block 3.0 (or higher) shares on a file server. The file server hosts the file shares. If you don't install the update on both machine roles, backup operations carried out by applications, which previously worked, might fail. For such failure scenarios, the Microsoft File Server Shadow Copy Agent Service will log FileShareShadowCopyAgent event 1013 on the file server. For more information, see KB5015527.	KB5014738	Applicable on Tim device

2022-06 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 for x64	This security update addresses an issue where a local user opening a specially crafted file could cause a denial of service condition on an affected system. For more information please see CVE-2022-30130.	KB5014808
Windows Malicious Software Removal Tool x64 - v5.102	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 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.	KB890830
2022-06 Cumulative Update for Windows Server 2016 for x64-based Systems	This security update includes quality improvements. Key changes include: Provides a Group Policy that administrators can use to enable customers to use the Ctrl+S (Save As) keyboard shortcut in Microsoft Edge IE Mode. Addresses an issue that prevents printing from operating properly for some low integrity process apps.	KB5014702

	Addresses an issue that causes print failures when a low integrity level (LowIL) application prints to a null port. Addresses an issue that prevents you from signing in to Citrix servers that have enabled the Interactive logon: Require smart card security policy setting. Addresses an issue that causes a mismatch between a Remote Desktop session's keyboard and the Remote Desktop Protocol (RDP) client when signing in. Addresses an issue that prevents the file system control code (FSCTL_SET_INTEGRITY_INFORMATION_EX) from handling its input parameter correctly. Addresses an elevation of privilege (EOP) vulnerability under CVE-2022-30154 for the Microsoft File Server Shadow Copy Agent Service. To become protected and functional, you must install the June 14, 2022 or later Windows update on both the application server and the file server. The application server runs the Volume Shadow Copy Service (VSS)-aware application that stores data on the remote Server Message Block 3.0 (or higher) shares on a file server. The file server hosts the file shares. If you don't install the update on both machine roles, backup operations carried out by applications, which previously worked, might fail. For such failure scenarios, the Microsoft File Server Shadow Copy Agent Service will log FileShareShadowCopyAgent event 1013 on the file server. For more information, see KB5015527.	
2022-06 Cumulative Update for .NET Framework 4.8 for Windows Server 2016 for x64	There are no new security improvements in this release. This update is cumulative and contains all previously released security improvements. This security update includes quality improvements. Key changes include:	KB5014630

2022-06 Cumulative Update for Windows Server 2016 for x64-based Systems	Provides a Group Policy that administrators can use to enable customers to use the Ctrl+S (Save As) keyboard shortcut in Microsoft Edge IE Mode. Addresses an issue that prevents printing from operating properly for some low integrity process apps. Addresses an issue that causes print failures when a low integrity level (LowIL) application prints to a null port. Addresses an issue that prevents you from signing in to Citrix servers that have enabled the Interactive logon: Require smart card security policy setting. Addresses an issue that causes a mismatch between a Remote Desktop session's keyboard and the Remote Desktop Protocol (RDP) client when signing in.	KB5014702

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.

Security Patches: PARx

June 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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
2022-06 Cumulative Update for Windows 10 Version 1607 for x64-based Systems (KB5014702)	This security update includes quality improvements. Key changes include: Provides a Group Policy that administrators can use to enable customers to use the Ctrl+S (Save As) keyboard shortcut in Microsoft Edge IE Mode. Addresses an issue that prevents printing from operating properly for some low integrity process apps. Addresses an issue that causes print failures when a low integrity level (LowIL) application prints to a null port. Addresses an issue that prevents you from signing in to Citrix servers that have enabled the Interactive logon: Require smart card security policy setting. Addresses an issue that causes a mismatch between a Remote Desktop session's keyboard and the Remote Desktop Protocol (RDP) client when signing in. Addresses an issue that prevents the file system control code (FSCTL_SET_INTEGRITY_INFORMATION_EX) from handling its input parameter correctly.	KB5014702	Applicable on Parx device.

Addresses an elevation of privilege (EOP) vulnerability under CVE-2022-30154 for the Microsoft File Server Shadow Copy Agent Service. To become protected and functional, you must install the June 14, 2022 or later Windows update on both the application server and the file server. The application server runs the Volume Shadow Copy Service (VSS)-aware application that stores data on the remote Server Message Block 3.0 (or higher) shares on a file server. The file server hosts the file shares. If you don't install the update on both machine roles, backup operations carried out by applications, which previously worked, might fail. For such failure scenarios, the Microsoft File Server Shadow Copy Agent Service will log FileShareShadowCopyAgent event 1013 on the file server. For more information, see KB5015527.

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.

Security Patches: BD Pyxis Connect

June 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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 - v5.102 (KB890830)	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	
2022-06 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 for x64 (KB5014808)	This security update addresses an issue where a local user opening a specially crafted file could cause a denial of service condition on an affected system.	KB5014808	

2022-06 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5014738)	It contains improvements and fixes, and addresses the following issues: - Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures. - Addresses an elevation of privilege (EOP) vulnerability under CVE-2022-30154 for the Microsoft File Server Shadow Copy Agent Service. To become protected and functional, you must install the June 14, 2022 or later Windows update on both the application server and the file server. The application server runs the Volume Shadow Copy Service (VSS)-aware application that stores data on the remote Server Message Block 3.0 (or higher) shares on a file server. The file server hosts the file shares. If you don't install the update on both machine roles, backup operations carried out by applications, which previously worked, might fail. For such failure scenarios, the Microsoft File Server Shadow Copy Agent Service will log FileShareShadowCopyAgent event 1013 on the file server.	KB5014738
2022-06 Cumulative Update for .NET Framework 4.8 for Windows Server 2016 for x64 (KB5014630)	There are no new security improvements in this release. This update is cumulative and contains all previously released security improvements. Quality and reliability improvements WPF1- Addresses an issue where DWM failures can cause WPF's render thread to fail. An app can opt-in to the behavior of ignoring all DwmFlush errors by setting a regkey in HKCU\Software\Microsoft\Avalon.Graphics\IgnoreDwmFlushErrors or HKLM\Software\Microsoft\Avalon.Graphics\IgnoreDwmFlushErrors whose name is the full path to the .exe that wants to opt-in, and whose DWORD value is 1. - Addresses an issue of WPF apps not working with "Text Cursor Indicator" enabled when using RichTextBox. Winforms - Improved the hardened rendering of ComboBox controls on 64 bit architectures. - Improved the reliability of data-bound ComboBox controls under assistive technology. .NET Runtime - Addresses several issues that would cause too many garbage collections under high memory load. The part of the change that reduces the number of blocking generation 2	KB5014630

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

	collections under high memory load is considered a tuning change and is only active if the GCConserveMemory setting is set to a non-zero value. The part of the change that reduces needless generation 0 collections is considered an improvement and is always active. - Adjusted GC Heap Hard Limit configuration, as well as processor interpretation for .NET Framework container scenarios. Workflow - Addresses an issue when users interact with the Workflow Designer they might encounter incorrectly disabled context menu items when right clicking on a variable in the component variables list.	
2022-06 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5014702)	It resolves zero-day and critical vulnerabilities published in June 2022. Besides the security vulnerability, KB5014702 also addresses a lot of bug fixes on Windows Server 2016.	KB5014702

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.

2022-06 Cumulative Update for Windows 10 Version 21H2 for x86-based Systems (KB5014699)	In addition to security fixes, Windows 10's June update also fixes an issue that prevents Microsoft Excel or Microsoft Outlook from opening.	KB5014699

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.

Security Patches: BD FHIR

June 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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
2022-06 Cumulative update for windows server 2019 for x64 based systems (KB5014692)	This security update includes improvements that were a part of update KB5014022 (released May 24, 2022) and also addresses the following issues: Addresses an elevation of privilege (EOP) vulnerability under CVE-2022-30154 for the Microsoft File Server Shadow Copy Agent Service. If we don't install the update on both machine roles, backup operations carried out by applications, which previously worked, might fail. If we installed earlier updates, only the new updates contained in this package will be downloaded and installed on your device.	KB5014692
2022-06 Cumulative update for .NET framework 3.5, 4.7.2 and 4.8 for Windows server 2019 x64 (KB5014805)	This update includes cumulative reliability improvements in .NET Framework 3.5 and 4.7.2. It is recommended to apply this update as part of our regular maintenance routines.	KB5014805
Security update for SQL server 2019 RTM GDR (KB5014356)	This security update includes security from an authenticated attacker that could affect SQL Server memory when executing a specially crafted query using $partition against a table with a Column Store index. The SQL Server components are updated to the following builds in this security update : SQL Server - Product version: 15.0.2095.3, file version: 2019.150.2095.3	KB5014356

Update for windows defender antivirus malware platform (KB4052623)	This update changes the antimalware client version. Version 4.18.2203.5 is re-released to prevent supersedence. Keeping Microsoft Defender Antivirus up to date is critical to assure your devices have the latest technology and features needed to protect against new malware and attack techniques.	KB4052623
Security update for microsoft ASP .net MVC 5.0 (KB2992080)	A security issue (MS14-059) has been identified in a Microsoft software product that could affect our system. we can protect our system by installing this update from Microsoft.	KB2992080
Security update for microsoft visual C++ 2008 service pack 1 redistributable package (KB2538243)	This security update resolves a publicly disclosed vulnerability in certain applications built using the Microsoft Foundation Class (MFC) Library.	KB2538243
Cumulative update for .NET framework 3.5, 4.7.2 and 4.8 for windows server 2019 for x64 (KB5013868)	This security update addresses an issue where a local user opening a specially crafted file could cause a denial of service condition on an affected system.	KB5013868

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.

Security Patches: BD Pyxis™ IV Prep

June 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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
2022-06 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5014746	Applicable on Cato
2022-06 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems	**A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.**	KB5014738	Applicable on Cato

Windows Malicious Software Removal Tool x64 - v5.102	**After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.**	KB890830	Applicable on Cato
2022-06 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 for x64	**Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.**	KB5014808	Applicable on Cato
Security Update for SQL Server 2014 Service Pack 3 GDR	**Security issues have been identified in the SQL Server 2014 Service Pack 3 GDR that could allow an attacker to compromise your system and gain control over it. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer.**	KB5014165	Applicable on Cato
2022-06 Cumulative Update for Windows Server 2016 for x64-based Systems	**A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.**	KB5014702	Applicable on Cato

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.

Security Patches: BD Pyxis™ Supply

June 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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
2022-06 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5014738)	This cumulative security update includes improvements that are part of update KB5014011 (released May 10, 2022) and includes new improvements for the following issue: • Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures. • Addresses an elevation of privilege (EOP) vulnerability under CVE-2022-30154 for the Microsoft File Server Shadow Copy Agent Service. To become protected and functional, you must install the June 14, 2022 or later Windows update on both the application server and the file server. The application server runs the Volume Shadow Copy Service (VSS)-aware application that stores data on the remote Server Message Block 3.0 (or higher) shares on a file server. The file server hosts the file shares. If you don't install the update on both machine roles, backup operations carried out by applications, which previously worked, might fail. For such failure scenarios, the Microsoft File Server Shadow Copy Agent Service will log FileShareShadowCopyAgent event 1013 on the file server. For more information, see KB5015527.	KB5014738	Applicable on Supply.

2022-06 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5014746)	This security-only update includes new improvements for the following issue: • Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures. • Addresses an elevation of privilege (EOP) vulnerability under CVE-2022-30154 for the Microsoft File Server Shadow Copy Agent Service. To become protected and functional, you must install the June 14, 2022 or later Windows update on both the application server and the file server. The application server runs the Volume Shadow Copy Service (VSS)-aware application that stores data on the remote Server Message Block 3.0 (or higher) shares on a file server. The file server hosts the file shares. If you don't install the update on both machine roles, backup operations carried out by applications, which previously worked, might fail. For such failure scenarios, the Microsoft File Server Shadow Copy Agent Service will log FileShareShadowCopyAgent event 1013 on the file server. For more information, see KB5015527.	KB5014746	Applicable on Supply.
2022-06 Security Only Quality Update for Windows Embedded Standard 7 for x64-based Systems (KB5014742)	This security-only update includes new improvements for the following issue: • Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures.	KB5014742	Applicable on Supply.

2022-06 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x64-based Systems (KB5014748)	This cumulative security update contains improvements that are part of update KB5014012 (released May 10, 2022) and includes new improvements for the following issue: • Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures.	KB5014748	Applicable on Supply.
2022-06 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5014702)	This security update includes quality improvements. Key changes include: • Provides a Group Policy that administrators can use to enable customers to use the Ctrl+S (Save As) keyboard shortcut in Microsoft Edge IE Mode. • Addresses an issue that prevents printing from operating properly for some low integrity process apps. • Addresses an issue that causes print failures when a low integrity level (LowIL) application prints to a null port. • Addresses an issue that prevents you from signing in to Citrix servers that have enabled the Interactive logon: Require smart card security policy setting. • Addresses an issue that causes a mismatch between a Remote Desktop session's keyboard and the Remote Desktop Protocol (RDP) client when signing in. • Addresses an issue that prevents the file system control code (FSCTL_SET_INTEGRITY_INFORMATION_EX) from handling its input parameter correctly. • Addresses an elevation of privilege (EOP) vulnerability under CVE-2022-30154 for the Microsoft File Server Shadow Copy Agent Service. To become protected and functional, you must install the June 14, 2022 or later Windows update on both the application server and the file server. The application server runs the Volume Shadow Copy Service (VSS)-aware application that stores data on the remote Server Message Block 3.0 (or higher) shares on a file server. The file server hosts the file shares. If you don't install the update on both machine roles, backup operations carried out by applications, which	KB5014702	Applicable on Supply.

	previously worked, might fail. For such failure scenarios, the Microsoft File Server Shadow Copy Agent Service will log FileShareShadowCopyAgent event 1013 on the file server. For more information, see KB5015527.		
2022-06 Cumulative Update for Windows 10 Version 1607 for x64-based Systems (KB5014702)	This security update includes quality improvements. Key changes include: • Provides a Group Policy that administrators can use to enable customers to use the Ctrl+S (Save As) keyboard shortcut in Microsoft Edge IE Mode. • Addresses an issue that prevents printing from operating properly for some low integrity process apps. • Addresses an issue that causes print failures when a low integrity level (LowIL) application prints to a null port. • Addresses an issue that prevents you from signing in to Citrix servers that have enabled the Interactive logon: Require smart card security policy setting. • Addresses an issue that causes a mismatch between a Remote Desktop session's keyboard and the Remote Desktop Protocol (RDP) client when signing in. • Addresses an issue that prevents the file system control code (FSCTL_SET_INTEGRITY_INFORMATION_EX) from handling its input parameter correctly. • Addresses an elevation of privilege (EOP) vulnerability under CVE-2022-30154 for the Microsoft File Server Shadow Copy Agent Service. To become protected and functional, you must install the June 14, 2022 or later Windows update on both the application server and the file server. The application server runs the Volume Shadow Copy Service (VSS)-aware application that stores data on the remote Server Message Block 3.0 (or higher) shares on a file server. The file server hosts the file shares. If you don't install the update on both machine roles, backup operations carried out by applications, which previously worked, might fail. For such failure scenarios, the Microsoft File Server Shadow Copy Agent Service will log FileShareShadowCopyAgent event 1013 on	KB5014702	Applicable on Supply.

	the file server. For more information, see KB5015527.		
2022-06 Cumulative Update for Windows Server 2019 for x64-based Systems (KB5014692)	This security update includes improvements that were a part of update KB5014022 (released May 24, 2022) and also addresses the following issues: • Addresses an elevation of privilege (EOP) vulnerability under CVE-2022-30154 for the Microsoft File Server Shadow Copy Agent Service. To become protected and functional, you must install the June 14, 2022 or later Windows update on both the application server and the file server. The application server runs the Volume Shadow Copy Service (VSS)-aware application that stores data on the remote Server Message Block 3.0 (or higher) shares on a file server. The file server hosts the file shares. If you don't install the update on both machine roles, backup operations carried out by applications, which previously worked, might fail. For such failure scenarios, the Microsoft File Server Shadow Copy Agent Service will log FileShareShadowCopyAgent event 1013 on the file server. For more information, see KB5015527.	KB5014692	Applicable on Supply.

2022-06 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB5014692)	**This security update includes improvements that were a part of update KB5014022 (released May 24, 2022) and also addresses the following issues:** • **Addresses an elevation of privilege (EOP) vulnerability under CVE-2022-30154 for the Microsoft File Server Shadow Copy Agent Service. To become protected and functional, you must install the June 14, 2022 or later Windows update on both the application server and the file server. The application server runs the Volume Shadow Copy Service (VSS)-aware application that stores data on the remote Server Message Block 3.0 (or higher) shares on a file server. The file server hosts the file shares. If you don't install the update on both machine roles, backup operations carried out by applications, which previously worked, might fail. For such failure scenarios, the Microsoft File Server Shadow Copy Agent Service will log FileShareShadowCopyAgent event 1013 on the file server. For more information, see KB5015527.**	**KB5014692**	**Applicable on Supply.**
Windows Malicious Software Removal Tool x64 - v5.102	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers. 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.	KB890830	Applicable on Supply.

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.

Security Patches: BD Pyxis™ CIISafe ES

June 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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 - v5.102	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	Applicable on CIIsafe device.
2022-06 Cumulative Update for Windows 10 Version 1809 for x64-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5014692	Applicable on CIIsafe device.

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.

Security Patches:
BD Pyxis™ Anesthesia ES

June 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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 - v5.102	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	Applicable on PAS device.
2022-06 Cumulative Update for Windows 10 Version 1809 for x64-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5014692	Applicable on PAS device.

2022-06 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems.	This cumulative security update contains improvements that are part of update KB5014012 (released May 10, 2022) and includes new improvements for the following issue: Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures.	KB5014748	Applicable on PAS device.
2022-06 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems.	This security-only update includes new improvements for the following issue: Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures.	KB5014742	Applicable on PAS device.
2022-06 Cumulative Update for Windows 10 Version 1607 for x64-based Systems.	This security update includes quality improvements. Key changes include: Provides a Group Policy that administrators can use to enable customers to use the Ctrl+S (Save As) keyboard shortcut in Microsoft Edge IE Mode. Addresses an issue that prevents printing from operating properly for some low integrity process apps. Addresses an issue that causes print failures when a low integrity level (LowIL) application prints to a null port. Addresses an issue that prevents you from signing in to Citrix servers that have enabled the Interactive logon: Require smart card security policy setting. Addresses an issue that causes a mismatch between a Remote Desktop session's keyboard and the Remote Desktop Protocol (RDP) client when signing in. Addresses an issue that prevents the file system control code (FSCTL_SET_INTEGRITY_INFORMATION_EX) from handling its input parameter correctly. Addresses an elevation of privilege (EOP) vulnerability under CVE-2022-30154 for the Microsoft File Server Shadow Copy Agent Service. To become protected and functional, you must install the June 14, 2022 or later Windows update on both the application server and the file server. The application server runs the Volume Shadow Copy Service (VSS)-aware application that stores data on the remote Server Message Block 3.0 (or higher) shares on a file server. The file server hosts the file shares. If you don't install the update on both machine roles, backup operations carried out by applications, which previously worked, might fail.	KB5014702	Applicable on PAS device.

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.

Security Patches:
BD Pyxis™ MedStation™ 4000

June 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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 - v5.102	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS4000 Console, Anesthesia System and Station
2022-06 Cumulative Update for Windows Server 2016 for x64-based Systems.	This security update includes quality improvements. Key changes include: Provides a Group Policy that administrators can use to enable customers to use the Ctrl+S (Save As) keyboard shortcut in Microsoft Edge IE Mode. Addresses an issue that prevents printing from operating properly for some low integrity process apps. Addresses an issue that causes print failures when a low integrity level (LowIL) application prints to a null port. Addresses an issue that prevents you from signing in to Citrix servers that have enabled the Interactive logon: Require smart card security policy setting. Addresses an issue that causes a mismatch between a Remote Desktop session's keyboard and the Remote Desktop Protocol (RDP) client when signing in. Addresses an issue that prevents the file system control code (FSCTL_SET_INTEGRITY_INFORMATION_EX) from handling its input parameter correctly. Addresses an elevation of privilege (EOP) vulnerability under CVE-2022-30154 for the Microsoft File Server Shadow Copy Agent Service. To become protected and functional, you must install the June 14, 2022 or later Windows update on both the application server and the file server. The application server runs the Volume Shadow Copy Service (VSS)-aware application that stores data on the remote Server Message Block	KB5014702	Applicable on MS4000 Console

	3.0 (or higher) shares on a file server. The file server hosts the file shares. If you don't install the update on both machine roles, backup operations carried out by applications, which previously worked, might fail. For such failure scenarios, the Microsoft File Server Shadow Copy Agent Service will log FileShareShadowCopyAgent event 1013 on the file server. For more information, see KB5015527.		
2022-06 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	This security update includes quality improvements. Key changes include: Provides a Group Policy that administrators can use to enable customers to use the Ctrl+S (Save As) keyboard shortcut in Microsoft Edge IE Mode. Addresses an issue that prevents printing from operating properly for some low integrity process apps. Addresses an issue that causes print failures when a low integrity level (LowIL) application prints to a null port. Addresses an issue that prevents you from signing in to Citrix servers that have enabled the Interactive logon: Require smart card security policy setting. Addresses an issue that causes a mismatch between a Remote Desktop session's keyboard and the Remote Desktop Protocol (RDP) client when signing in. Addresses an issue that prevents the file system control code (FSCTL_SET_INTEGRITY_INFORMATION_EX) from handling its input parameter correctly. Addresses an elevation of privilege (EOP) vulnerability under CVE-2022-30154 for the Microsoft File Server Shadow Copy Agent Service. To become protected and functional, you must install the June 14, 2022 or later Windows update on both the application server and the file server. The application server runs the Volume Shadow Copy Service (VSS)-aware application that stores data on the remote Server Message Block 3.0 (or higher) shares on a file server. The file server hosts the file shares. If you don't install the update on both machine roles, backup operations carried out by applications, which previously worked, might fail. For such failure scenarios, the Microsoft File Server Shadow Copy Agent Service will log FileShareShadowCopyAgent event 1013 on the file server. For more information, see KB5015527.	KB5014702	Applicable on MS4000 and Anesthesia System
Windows Malicious Software Removal Tool - v5.102	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS4000 Console and MED3500 Console

2022-06 Security Only Quality Update for Windows Server 2008 for x86-based Systems.	This security-only update includes new improvements for the following issue: Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures.	KB5014743	Applicable on MS4000 Console and MED3500 Console
2022-06 Security Monthly Quality Rollup for Windows Server 2008 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5014010 (released May 10, 2022) and includes new improvements for the following issue: Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures.	KB5014752	Applicable on MS4000 Console and MED3500 Console
2022-06 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5014012 (released May 10, 2022) and includes new improvements for the following issue: Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures.	KB5014748	Applicable on MS4000 and Anesthesia System
2022-06 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This security-only update includes new improvements for the following issue: Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures.	KB5014742	Applicable on MS4000 and Anesthesia System

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.

Security Patches:
BD Pyxis™ MedStation™ 3500

June 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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
2022-06 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems.	This cumulative security update contains improvements that are part of update KB5014012 (released May 10, 2022) and includes new improvements for the following issue: Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures.	KB5014748	Applicable on 3500 Anesthesia System and MS3500 Station
2022-06 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems.	This security-only update includes new improvements for the following issue: Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures.	KB5014742	Applicable on 3500 Anesthesia System and MS3500 Station
Windows Malicious Software Removal Tool - v5.102	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS3500 and MS 4000 Console

2022-06 Security Only Quality Update for Windows Server 2008 for x86-based Systems.	This security-only update includes new improvements for the following issue: Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures.	KB5014743	Applicable on MS3500 and MS 4000 Console
2022-06 Security Monthly Quality Rollup for Windows Server 2008 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5014010 (released May 10, 2022) and includes new improvements for the following issue: Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures.	KB5014752	Applicable on MS3500 and MS 4000 Console

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.

Security Patches:
BD Pyxis™ Anesthesia System 4000

June 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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 - v5.102	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS4000 Console, Anesthesia System and Station
2022-06 Cumulative Update for Windows 10 Version 1607 for x64-based Systems.	This security update includes quality improvements. Key changes include: Provides a Group Policy that administrators can use to enable customers to use the Ctrl+S (Save As) keyboard shortcut in Microsoft Edge IE Mode. Addresses an issue that prevents printing from operating properly for some low integrity process apps. Addresses an issue that causes print failures when a low integrity level (LowIL) application prints to a null port. Addresses an issue that prevents you from signing in to Citrix servers that have enabled the Interactive logon: Require smart card security policy setting. Addresses an issue that causes a mismatch between a Remote Desktop session's keyboard and the Remote Desktop Protocol (RDP) client when signing in. Addresses an issue that prevents the file system control code (FSCTL_SET_INTEGRITY_INFORMATION_EX) from handling its input parameter correctly. Addresses an elevation of privilege (EOP) vulnerability under CVE-2022-30154 for the Microsoft File Server Shadow Copy Agent Service. To become protected and functional, you must	KB5014702	Applicable on Anesthesia System and MS4000

	install the June 14, 2022 or later Windows update on both the application server and the file server. The application server runs the Volume Shadow Copy Service (VSS)-aware application that stores data on the remote Server Message Block 3.0 (or higher) shares on a file server. The file server hosts the file shares. If you don't install the update on both machine roles, backup operations carried out by applications, which previously worked, might fail. For such failure scenarios, the Microsoft File Server Shadow Copy Agent Service will log FileShareShadowCopyAgent event 1013 on the file server. For more information, see KB5015527.		
2022-06 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems.	This cumulative security update contains improvements that are part of update KB5014012 (released May 10, 2022) and includes new improvements for the following issue: Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures.	KB5014748	Applicable on Anesthesia System and MS4000
2022-06 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This security-only update includes new improvements for the following issue: Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures.	KB5014742	Applicable on Anesthesia System and Station

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.

Security Patches:
BD Pyxis™ Anesthesia System 3500

June 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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
2022-06 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems.	This cumulative security update contains improvements that are part of update KB5014012 (released May 10, 2022) and includes new improvements for the following issue: Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures.	KB5014748	Applicable on 3500 Anesthesia System and MS3500 Station
2022-06 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems.	This security-only update includes new improvements for the following issue: Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures.	KB5014742	Applicable on 3500 Anesthesia System and MS3500 Station

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.

Security Patches: Security Module

June 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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 - v5.102 (KB890830)	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	Applicable on Security Module devices.

2022-06 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5014738)	This cumulative security update includes improvements that are part of update KB5014011 (released May 10, 2022) and includes new improvements for the following issue: • Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures. • Addresses an elevation of privilege (EOP) vulnerability under CVE-2022-30154 for the Microsoft File Server Shadow Copy Agent Service. To become protected and functional, you must install the June 14, 2022 or later Windows update on both the application server and the file server. The application server runs the Volume Shadow Copy Service (VSS)-aware application that stores data on the remote Server Message Block 3.0 (or higher) shares on a file server. The file server hosts the file shares. If you don't install the update on both machine roles, backup operations carried out by applications, which previously worked, might fail. For such failure scenarios, the Microsoft File Server Shadow Copy Agent Service will log FileShareShadowCopyAgent event 1013 on the file server.	KB5014738	Applicable on Security Module devices.
2022-06 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5014746)	This security-only update includes new improvements for the following issue: • Printing to a NUL port from a Low Integrity Level (LowIL) process application could cause printing failures. • Addresses an elevation of privilege (EOP) vulnerability under CVE-2022-30154 for the Microsoft File Server Shadow Copy Agent Service. To become protected and functional, you must install the June 14, 2022 or later Windows update on both the application server and the file server. The application server runs the Volume Shadow Copy Service (VSS)-aware application that stores data on the remote Server Message Block 3.0 (or higher) shares on a file server. The file server hosts the file shares. If you don't install the update on both machine roles, backup operations carried out by applications, which previously worked, might fail. For such failure scenarios, the Microsoft File Server Shadow Copy Agent Service will log FileShareShadowCopyAgent event 1013 on the file server.	KB5014746	Applicable on Security Module devices.

2022-06 Cumulative Update for Windows 10 Version 1607 for x64-based Systems (KB5014702)	This security update includes quality improvements. Key changes include: • Provides a Group Policy that administrators can use to enable customers to use the Ctrl+S (Save As) keyboard shortcut in Microsoft Edge IE Mode. • Addresses an issue that prevents printing from operating properly for some low integrity process apps. • Addresses an issue that causes print failures when a low integrity level (LowIL) application prints to a null port. • Addresses an issue that prevents you from signing in to Citrix servers that have enabled the Interactive logon: Require smart card security policy setting. • Addresses an issue that causes a mismatch between a Remote Desktop session's keyboard and the Remote Desktop Protocol (RDP) client when signing in. • Addresses an issue that prevents the file system control code (FSCTL_SET_INTEGRITY_INFORMATION_EX) from handling its input parameter correctly. • Addresses an elevation of privilege (EOP) vulnerability under CVE-2022-30154 for the Microsoft File Server Shadow Copy Agent Service. To become protected and functional, you must install the June 14, 2022 or later Windows update on both the application server and the file server. The application server runs the Volume Shadow Copy Service (VSS)-aware application that stores data on the remote Server Message Block 3.0 (or higher) shares on a file server. The file server hosts the file shares. If you don't install the update on both machine roles, backup operations carried out by applications, which previously worked, might fail. For such failure scenarios, the Microsoft File Server Shadow Copy Agent Service will log FileShareShadowCopyAgent event 1013 on the file server.	KB5014702	Applicable on Security Module devices.

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.