Security Patches: BD Pyxis CIISafe

June 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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
Windows Malicious Software Removal Tool x64 - v5.114 (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 to CII safe devices.

2023-06 Cumulative Update for Windows 10 Version 1607 for x64-based Systems (KB5027219)	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 june have to restart your system.	KB5027219	Applicable to CII safe devices.
2023-06 Cumulative Update for .NET Framework 4.8 for Windows 10 Version 1607 for x64 (KB5027123)	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 june have to restart your system.	KB5027123	Applicable to CII safe devices.
2023-06 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems (KB5027275)	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 june have to restart your system.	KB5027275	Applicable to CII safe devices.
2023-06 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems (KB5027256)	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 june have to restart your system.	KB5027256	Applicable to CII safe devices.
2023-06 Security Only Update for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7	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 june have to restart your system.	KB5027531	Applicable to CII safe devices.

2023-06 Security and Quality Rollup for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7 (KB5027540)	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 june have to restart your system.	KB5027540	Applicable to CII safe devices.

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

bd.com

Security Patches: BD Pyxis™ Anesthesia System 4000

June 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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
Windows Malicious Software Removal Tool x64 - v5.114	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS4000 Console and 4000 Anesthesia and Station
2023-06 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	This security update includes quality improvements. When you install this KB: ▪ This update addresses an issue that might cause a memory leak. The leak might occur during prolonged Remote Desktop audio redirection. ▪ This update addresses an issue that affects the Windows Kernel. This issue is related to CVE-2023-32019. To learn more, see KB5028407.This update addresses an issue that affects Microsoft Edge IE mode. The issue stops you from configuring add-ons.	KB5027219	Applicable on 4000 Anesthesia System and MS4000 Station
2023-06 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This update contains miscellaneous security improvements to internal Windows OS functionality. No additional issues were documented for this release.	KB5027256	Applicable on 4000 Anesthesia System and 4000 Station

2023-06 Security and Quality Rollup for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7	This security update addresses a vulnerability in the MSDIA SDK where corrupted PDBs can cause heap overflow, leading to a crash or remove code execution. This security update addresses a vulnerability in WPF where the BAML offers other ways to instantiate types that leads to an elevation of privilege. This security update addresses a vulnerability in the WPF XAML parser where an unsandboxed parser can lead to remote code execution This security update addresses a vulnerability in bypass restrictions when deserializing a DataSet or DataTable from XML, leading to an elevation of privilege.	KB5027540	Applicable on 4000 Anesthesia System and 4000 Station
2023-06 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5026413 (released May 9, 2023). This update also contains miscellaneous security improvements to internal Windows OS functionality. No specific issues are documented for this release.	KB5027275	Applicable on 4000 Anesthesia System and 4000 Station
2023-06 Security Only Update for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7	This security update addresses a vulnerability in the MSDIA SDK where corrupted PDBs can cause heap overflow, leading to a crash or remove code execution. This security update addresses a vulnerability in WPF where the BAML offers other ways to instantiate types that leads to an elevation of privilege. This security update addresses a vulnerability in the WPF XAML parser where an unsandboxed parser can lead to remote code execution.	KB5027531	Applicable on 4000 Anesthesia System and 4000 Station

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

bd.com

Security Patches: BD Pyxis™ MedStation™ 4000

June 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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
Windows Malicious Software Removal Tool x64 - v5.114	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS4000 Console and 4000 Anesthesia and Station
2023-06 Cumulative Update for Windows Server 2016 for x64-based System	This security update includes quality improvements. When you install this KB: ▪ This update addresses an issue that might cause a memory leak. The leak might occur during prolonged Remote Desktop audio redirection. ▪ This update addresses an issue that affects the Windows Kernel. This issue is related to CVE-2023-32019. To learn more, see KB5028407.	KB5027219	Applicable on MS4000 Console
2023-06 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	This security update includes quality improvements. When you install this KB: ▪ This update addresses an issue that might cause a memory leak. The leak might occur during prolonged Remote Desktop audio redirection. ▪ This update addresses an issue that affects the Windows Kernel. This issue is related to CVE-2023-32019. To learn more, see KB5028407.This update addresses an issue that affects Microsoft Edge IE mode. The issue stops you from configuring add-ons.	KB5027219	Applicable on 4000 Anesthesia System and MS4000 Station
Windows Malicious Software Removal Tool - v5.114	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS4000 Console

2023-06 Security Only Quality Update for Windows Server 2008 for x86-based Systems	This update contains miscellaneous security improvements to internal Windows OS functionality. No additional issues were documented for this release.	KB5027277	Applicable on MS4000 Console
2023-06 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This update contains miscellaneous security improvements to internal Windows OS functionality. No additional issues were documented for this release.	KB5027256	Applicable on 4000 Anesthesia System and 4000 Station
2023-06 Security and Quality Rollup for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7	This security update addresses a vulnerability in the MSDIA SDK where corrupted PDBs can cause heap overflow, leading to a crash or remove code execution. This security update addresses a vulnerability in WPF where the BAML offers other ways to instantiate types that leads to an elevation of privilege. This security update addresses a vulnerability in the WPF XAML parser where an unsandboxed parser can lead to remote code execution This security update addresses a vulnerability in bypass restrictions when deserializing a DataSet or DataTable from XML, leading to an elevation of privilege.	KB5027540	Applicable on 4000 Anesthesia System and 4000 Station
2023-06 Security Monthly Quality Rollup for Windows Server 2008 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5026408 (released May 9, 2023). This update also contains miscellaneous security improvements to internal Windows OS functionality. No specific issues are documented for this release.	KB5027279	Applicable on MS4000 Console
2023-06 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5026413 (released May 9, 2023). This update also contains miscellaneous security improvements to internal Windows OS functionality. No specific issues are documented for this release.	KB5027275	Applicable on 4000 Anesthesia System and 4000 Station
2023-06 Security Only Update for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7	This security update addresses a vulnerability in the MSDIA SDK where corrupted PDBs can cause heap overflow, leading to a crash or remove code execution. This security update addresses a vulnerability in WPF where the BAML offers other ways to instantiate types that leads to an elevation of privilege. This security update addresses a vulnerability in the WPF XAML parser where an unsandboxed parser can lead to remote code execution.	KB5027531	Applicable on 4000 Anesthesia System and 4000 Station

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

bd.com

Security Patches: Security Module

June 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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
Windows Malicious Software Removal Tool x64 - v5.114 (KB890830)	If malicious software has modified (infected) files on your computer, the tool prompts you to remove the malicious software from those files. If the malicious software modified your browser settings, your homepage may be changed automatically to a page that gives you directions on how to restore these settings.	KB890830	Applicable on Security Module devices.
2023-06 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB5027574)	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.	KB5027574	Applicable on Security Module devices.
2023-06 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5027282)	This update contains miscellaneous security improvements to internal Windows OS functionality.	KB5027282	Applicable on Security Module devices.
2023-06 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 for x64 (KB5027533)	This update makes changes for the following Vulnerabilities. .NET Framework Remote Code Execution Vulnerability .NET Framework Elevation of Privilege Vulnerability .NET Framework Denial of Service Vulnerability	KB5027533	Applicable on Security Module devices.
2023-06 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 (KB5027542)	This update makes changes for the following Vulnerabilities. .NET Framework Remote Code Execution Vulnerability .NET Framework Elevation of Privilege Vulnerability .NET Framework Denial of Service Vulnerability	KB5027542	Applicable on Security Module devices.

2023-06 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5027271)	This cumulative security update includes improvements that are part of update KB5026415 (released May 9, 2023). This update also contains miscellaneous security improvements to internal Windows OS functionality.	KB5027271	Applicable on Security Module devices.
2023-06 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5027219)	This security update includes following improvements. This update addresses an issue that might cause a memory leak. The leak might occur during prolonged Remote Desktop audio redirection. This update addresses an issue that affects the Windows Kernel.	KB5027219	Applicable on Security Module devices.

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

bd.com

Security Patches: BD Pyxis™ IV Prep

June 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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
Windows Malicious Software Removal Tool x64 - v5.114	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
2023-06 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems	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.	KB5027574	Applicable on Cato

2023-06 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.	KB5027282	Applicable on Cato
2023-06 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 for x64	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	KB5027533	Applicable on Cato
2023-06 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	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	KB5027542	Applicable on Cato
2023-06 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	KB5027271	Applicable on Cato
2023-06 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	KB5027219	Applicable on Cato

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

bd.com

Security Patches: BD Pyxis Connect

June 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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
2023-06 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB5027574)	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.	KB5027574	N/A
2023-06 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5027282)	This update contains miscellaneous security improvements to internal Windows OS functionality. No specific issues are documented for this release.	KB5027282	N/A
Windows Malicious Software Removal Tool x64 - v5.114 (KB890830)	Windows Malicious Software Removal Tool (MSRT) helps keep Windows computers free from prevalent malware. MSRT finds and removes threats and reverses the changes made by these threats. MSRT is generally released monthly as part of Windows Update or as a standalone tool.	KB890830	N/A

2023-06 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 for x64 (KB5027533)	This update makes following improvements: • CVE-2023-24897 - .NET Framework Remote Code Execution Vulnerability: This security update addresses a vulnerability in the MSDIA SDK where corrupted PDBs can cause heap overflow, leading to a crash or remove code execution. For more information see CVE 2023-24897. • CVE-2023-29326 - .NET Framework Remote Code Execution Vulnerability: This security update addresses a vulnerability in WPF where the BAML offers other ways to instantiate types that leads to an elevation of privilege. For more information see CVE-2023-29326. • CVE-2023-24895 - .NET Framework Remote Code Execution Vulnerability: This security update addresses a vulnerability in the WPF XAML parser where an unsandboxed parser can lead to remote code execution. For more information see CVE-2023-24895. • CVE-2023-24936 - .NET Framework Elevation of Privilege Vulnerability: This security update addresses a vulnerability in bypass restrictions when deserializing a DataSet or DataTable from XML, leading to an elevation of privilege. For more information see CVE-2023-24936. • CVE-2023-29331 - .NET Framework Denial of Service Vulnerability: This security update addresses a vulnerability where the AIA fetching process for client certificates can lead to denial of service. For more information see CVE 2023-29331. • CVE-2023-32030 - .NET Framework Denial of Service Vulnerability: This security update addresses a vulnerability where X509Certificate2 file handling can lead to denial of service. For more information see CVE 2023-32030.	KB5027533	N/A
2023-06 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 (KB5027542)	This update makes following improvements: • CVE-2023-24897 - .NET Framework Remote Code Execution Vulnerability: This security update addresses a vulnerability in the MSDIA SDK where corrupted PDBs can cause heap overflow, leading to a crash or remove code execution. For more information see CVE 2023-24897. • CVE-2023-29326 - .NET Framework Remote Code Execution Vulnerability: This security update addresses a vulnerability in WPF where the BAML offers other ways to	KB5027542	N/A

	instantiate types that leads to an elevation of privilege. For more information see CVE-2023-29326. • CVE-2023-24895 - .NET Framework Remote Code Execution Vulnerability: This security update addresses a vulnerability in the WPF XAML parser where an unsandboxed parser can lead to remote code execution. For more information see CVE-2023-24895. • CVE-2023-24936 - .NET Framework Elevation of Privilege Vulnerability: This security update addresses a vulnerability in bypass restrictions when deserializing a DataSet or DataTable from XML, leading to an elevation of privilege. For more information see CVE-2023-24936. • CVE-2023-29331 - .NET Framework Denial of Service Vulnerability: This security update addresses a vulnerability where the AIA fetching process for client certificates can lead to denial of service. For more information see CVE 2023-29331. • CVE-2023-32030 - .NET Framework Denial of Service Vulnerability: This security update addresses a vulnerability where X509Certificate2 file handling can lead to denial of service. For more information see CVE 2023-32030.		
2023-06 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5027219)	This security update includes following quality improvements: • Addresses an issue that might cause a memory leak. The leak might occur during prolonged Remote Desktop audio redirection. • Addresses an issue that affects the Windows Kernel. This issue is related to CVE-2023-32019. To learn more, see KB5028407.	KB5027219	
2023-06 Cumulative Update for .NET Framework 4.8 for Windows Server 2016 for x64 (KB5027123)	This security update includes cumulative security and reliability improvements in .NET Framework 4.8	KB5027123	

2023-06 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2 for x64 (KB5027538)	This security update includes the Cumulative Update for 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2.	KB5027538	
2023-06 Cumulative Update for Windows 10 Version 22H2 for x64-based Systems (KB5027215)	This update includes the primary goals of resolving known issues, addressing security vulnerabilities, and improving overall performance.	KB5027215	

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

bd.com

Security Patches: BD Pharmogistics

June 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for June 2023. 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.
2023-06 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5027219) Last Modified: 6/13/2023	This security update includes quality improvements. When you install this KB: This update addresses an issue that might cause a memory leak. The leak might occur during prolonged Remote Desktop audio redirection. This update addresses an issue that affects the Windows Kernel. This issue is related to CVE-2023-32019. To learn more, see KB5028407.	KB5027219	N/A

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

bd.com

2023-06 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (KB5027275) Last Modified: 6/13/2023	This cumulative security update contains improvements that are part of update KB5026413 (released May 9, 2023). This update also contains miscellaneous security improvements to internal Windows OS functionality. No specific issues are documented for this release.	KB5027275	N/A
2023-06 Security Only Quality Update for Windows Server 2008 R2 for x64-based Systems (KB5027256) Last Modified: 6/13/2023	This update contains miscellaneous security improvements to internal Windows OS functionality. No additional issues were documented for this release.	KB5027256	N/A
2023-06 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB5027574) Last Modified: 6/13/2023	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.	KB5027574	N/A

2023-06 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5027282) Last Modified: 6/13/2023	This update contains miscellaneous security improvements to internal Windows OS functionality. No specific issues are documented for this release.	KB5027282	N/A
2023-06 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 for x64 (KB5027533) Last Modified: 6/13/2023	CVE-2023-24897 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in the MSDIA SDK where corrupted PDBs can cause heap overflow, leading to a crash or remove code execution. CVE-2023-29326 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in WPF where the BAML offers other ways to instantiate types that leads to an elevation of privilege. CVE-2023-24895 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in the WPF XAML parser where an unsandboxed parser can lead to remote code execution. CVE-2023-24936 - .NET Framework Elevation of Privilege Vulnerability This security update addresses a vulnerability in bypass restrictions when deserializing a DataSet or DataTable from XML, leading to an elevation of privilege. CVE-2023-29331 - .NET Framework Denial of Service Vulnerability	KB5027533	N/A

	This security update addresses a vulnerability where the AIA fetching process for client certificates can lead to denial of service. CVE-2023-32030 - .NET Framework Denial of Service Vulnerability This security update addresses a vulnerability where X509Certificate2 file handling can lead to denial of service.		
2023-06 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 (KB5027542) Last Modified: 6/13/2023	CVE-2023-24897 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in the MSDIA SDK where corrupted PDBs can cause heap overflow, leading to a crash or remove code execution. CVE-2023-29326 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in WPF where the BAML offers other ways to instantiate types that leads to an elevation of privilege. CVE-2023-24895 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in the WPF XAML parser where an unsandboxed parser can lead to remote code execution. CVE-2023-24936 - .NET Framework Elevation of Privilege Vulnerability This security update addresses a vulnerability in bypass restrictions when deserializing a DataSet or DataTable from XML, leading to an elevation of privilege. CVE-2023-29331 - .NET Framework Denial of Service Vulnerability	KB5027542	N/A

	This security update addresses a vulnerability where the AIA fetching process for client certificates can lead to denial of service. CVE-2023-32030 - .NET Framework Denial of Service Vulnerability This security update addresses a vulnerability where X509Certificate2 file handling can lead to denial of service.		
2023-06 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5027271) Last Modified: 6/13/2023	This cumulative security update includes improvements that are part of update KB5026415 (released May 9, 2023). This update also contains miscellaneous security improvements to internal Windows OS functionality. No specific issues are documented for this release.	KB5027271	N/A
2023-06 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 21H2 for x64 (KB5027537) Last Modified: 6/13/2023	CVE-2023-24897 - .NET Framework Remote Code Execution Vulnerability CVE-2023-29326 - .NET Framework Remote Code Execution Vulnerability CVE-2023-24895 - .NET Framework Remote Code Execution Vulnerability CVE-2023-24936 - .NET Framework Elevation of Privilege Vulnerability CVE-2023-29331 - .NET Framework Denial of Service Vulnerability CVE-2023-32030 - .NET Framework Denial of Service Vulnerability	KB5027537	N/A

2023-06 Dynamic Cumulative Update for Windows 10 Version 21H2 for x64-based Systems (KB5027215) Last Modified: 6/13/2023	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) ensure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.	KB5027215	N/A

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

bd.com

Security Patches: PARx

June 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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
Windows Malicious Software Removal Tool x64 - v5.114	Windows Malicious Software Removal Tool (MSRT) 5.114 helps remove malicious software from computers running Windows11, Windows 10, Windows 8.1, Windows Server 2012 R2, Windows 8, Windows Server 2012, Windows 7, or Windows Server 2008.	KB890830	Applicable on ParX
2023-06 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	The remote Windows host is missing security update 5027219. It is, therefore, affected by multiple vulnerabilities - Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability (CVE-2023-29363, CVE-2023-32014, CVE-2023-32015) - Windows Collaborative Translation Framework Elevation of Privilege Vulnerability (CVE-2023-32009) - Microsoft ODBC Driver Remote Code Execution Vulnerability (CVE-2023-29373)	KB5027219	Applicable on ParX

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

bd.com

Security Patches: TIM

June 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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
2023-06 Cumulative Update for Windows Server 2016 for x64-based Systems	This security update includes quality improvements. When you install this KB: This update addresses an issue that might cause a memory leak. The leak might occur during prolonged Remote Desktop audio redirection. This update addresses an issue that affects the Windows Kernel. This issue is related to CVE-2023-32019. To learn more, see KB5028407. If you installed earlier updates, only the new updates contained in this package will be downloaded and installed on your device.	KB5027219	Applicable on TIM.
Windows Malicious Software Removal Tool x64 - v5.114	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	KB890830	Applicable on TIM.

	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. This article contains information about how the tool differs from an antivirus or antimalware product, how you can download and run the tool, what happens when the tool finds malware, and tool release information. It also includes information for the administrators and advanced users, including information about supported command-line switches.		
2023-06 Cumulative Update for .NET Framework 4.8 for Windows Server 2016 for x64	The June 13, 2023 update for Windows 10, version 1607 and Windows Server 2016 includes cumulative security and reliability improvements in .NET Framework 4.8. We recommend that you apply this update as part of your regular maintenance routines. Before you install this update, see the Prerequisites and Restart requirement sections.	KB5027123	Applicable on TIM.
2023-06 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.	KB5027574	Applicable on TIM.
2023-06 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems	This update contains miscellaneous security improvements to internal Windows OS functionality. No specific issues are documented for this release. For more information about the resolved security vulnerabilities, please refer to the Deployments l Security Update Guide and the June 2023 Security Updates.	KB5027282	Applicable on TIM.

2023-06 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 for x64	CVE-2023-24897 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in the MSDIA SDK where corrupted PDBs can cause heap overflow, leading to a crash or remove code execution. For more information see CVE 2023-24897. CVE-2023-29326 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in WPF where the BAML offers other ways to instantiate types that leads to an elevation of privilege. For more information see CVE-2023-29326. CVE-2023-24895 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in the WPF XAML parser where an unsandboxed parser can lead to remote code execution. For more information see CVE-2023-24895. CVE-2023-24936 - .NET Framework Elevation of Privilege Vulnerability This security update addresses a vulnerability in bypass restrictions when deserializing a DataSet or DataTable from XML, leading to an elevation of privilege. For more information see CVE-2023-24936. CVE-2023-29331 - .NET Framework Denial of Service Vulnerability This security update addresses a vulnerability where the AIA fetching process for client certificates can lead to denial of service. For more information see CVE 2023-29331. CVE-2023-29330 - .NET Framework Denial of Service Vulnerability This security update addresses a vulnerability where X509Certificate2 file handling can lead to denial of service. For more information see CVE 2023-32030.	**KB5027533**	Applicable on TIM.
2023-06 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	CVE-2023-24897 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in the MSDIA SDK where corrupted PDBs can cause heap overflow, leading to a crash or remove code execution. For more information see CVE 2023-24897.	KB5027542	Applicable on TIM.

	CVE-2023-29326 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in WPF where the BAML offers other ways to instantiate types that leads to an elevation of privilege. For more information see CVE-2023-29326. CVE-2023-24895 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in the WPF XAML parser where an unsandboxed parser can lead to remote code execution. For more information see CVE-2023-24895. CVE-2023-24936 - .NET Framework Elevation of Privilege Vulnerability This security update addresses a vulnerability in bypass restrictions when deserializing a DataSet or DataTable from XML, leading to an elevation of privilege. For more information see CVE-2023-24936.		
2023-06 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems	This cumulative security update includes improvements that are part of update KB5026415 (released May 9, 2023). This update also contains miscellaneous security improvements to internal Windows OS functionality. No specific issues are documented for this release. For more information about the resolved security vulnerabilities, please refer to the Deployments I Security Update Guide and the June 2023 Security Updates.	KB5027271	Applicable on TIM.

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

bd.com

Security Patches:
BD Pyxis™ ES Server

June 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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
2023-06 Cumulative Update for Windows Server 2019 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.	KB5027222	Applicable on 1.7.1.,1.7.2,1.7.3 ES Server.
2023-06 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64	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.	KB5027536	Applicable on 1.7.1.,1.7.2,1.7.3 ES Server.

Windows Malicious Software Removal Tool x64 - v5.114	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 1.7.1.,1.7.2,1.7.3 ES Server.

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

bd.com

Security Patches: BD Pyxis™ Anesthesia ES

June 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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
2023-06 Security Only Quality Update for Windows Embedded Standard 7 for x86-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.	KB5027256	Applicable on PAS device.
2023-06 Security and Quality Rollup for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7	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.	KB5027540	Applicable on PAS device.

Windows Malicious Software Removal Tool x64 - v5.114	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.
2023-06 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-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.	KB5027275	Applicable on PAS device.
2023-06 Security Only Update for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7	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.	KB5027531	Applicable on PAS device.

2023-06 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.	KB5027219	Applicable on PAS device.
2023-06 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.	KB5027222	Applicable on PAS device.
2023-06 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10 Version 1809	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.	KB5027536	Applicable on PAS device.

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

bd.com

Security Patches: BD Pyxis™ CIISafe ES

June 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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
2023-06 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.	KB5027222	Applicable on CIISafe device.
2023-06 Cumulative Update for Windows 10 Version 21H2 for x64-based Systems	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.	KB5027215	Applicable on CIISafe device.
2023-06 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10 Version 1809 for x64	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.	KB5027536	Applicable on CIISafe device.

2023-06 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 21H2 for x64	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.	KB5027537	Applicable on CIISafe device.
Windows Malicious Software Removal Tool x64 - v5.114	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.

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

bd.com

Security Patches: BD Pyxis™ Medstation ES

June 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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
2023-06 Security Only Quality Update for Windows Embedded Standard 7 for x86-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.	KB5027256	Applicable on Medstn ES device.
2023-06 Security and Quality Rollup for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7	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.	KB5027540	Applicable on Medstn ES device.

Windows Malicious Software Removal Tool x64 - v5.114	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 ES device.
2023-06 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-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.	KB5027275	Applicable on Medstn ES device.
2023-06 Security Only Update for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7	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.	KB5027531	Applicable on Medstn ES device.

2023-06 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.	KB5027219	Applicable on Medstn ES device.
2023-06 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.	KB5027222	Applicable on Medstn ES device.
2023-06 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10 Version 1809	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.	KB5027536	Applicable on Medstn ES device.

2023-06 Cumulative Update for .NET Framework 4.8 for Windows 10 Version 1607 for x64	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.	KB5027123	Applicable on Medstn ES device.

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

bd.com

Security Patches:
BD Pyxis™ Anesthesia ES

June 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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
2023-06 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.	KB5027222	Applicable on PAS 1.7.1.,1.7.2,1.7.3 device.
2023-06 Cumulative Update for Windows 10 Version 21H2 for x64-based Systems	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.	KB5027215	Applicable on PAS 1.7.1.,1.7.2,1.7.3 device.
2023-06 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10 Version 1809 for x64	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.	KB5027536	Applicable on PAS 1.7.1.,1.7.2,1.7.3 device.

2023-06 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 21H2 for x64	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.	KB5027537	Applicable on PAS 1.7.1.,1.7.2,1.7.3 device.
Windows Malicious Software Removal Tool x64 - v5.114	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 1.7.1.,1.7.2,1.7.3 device.

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

bd.com

Security Patches: BD Pyxis™ Medstation ES

June 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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
2023-06 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.	KB5027222	Applicable on 1.7.1.,1.7.2,1.7.3 MedSTN device.
2023-06 Cumulative Update for Windows 10 Version 21H2 for x64-based Systems	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.	KB5027215	Applicable on 1.7.1.,1.7.2,1.7.3 MedSTN device.
2023-06 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10 Version 1809 for x64	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.	KB5027536	Applicable on 1.7.1.,1.7.2,1.7.3 MedSTN device.

2023-06 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 21H2 for x64	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.	KB5027537	Applicable on 1.7.1.,1.7.2,1.7.3 MedSTN device.
Windows Malicious Software Removal Tool x64 - v5.114	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 1.7.1.,1.7.2,1.7.3 MedSTN device.

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

bd.com

Security Patches:
BD Pyxis™ MedES Server

June 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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
2023-06 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems	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.	KB5027574	Applicable on MedES Server.
2023-06 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.	KB5027282	Applicable on MedES Server.

2023-06 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 for x64	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.	KB5027533	Applicable on MedES Server.
2023-06 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	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.	KB5027542	Applicable on MedES Server.
2023-06 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.	KB5027271	Applicable on MedES Server.

Windows Malicious Software Removal Tool x64 - v5.114	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 MedES Server.

2023-06 Security Only Quality Update for Windows Server 2008 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.	KB5027277	Applicable on MedES Server.
2023-06 Security Monthly Quality Rollup for Windows Server 2008 for x86-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.	KB5027279	Applicable on MedES Server.

2023-06 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.	KB5027219	Applicable on Meds Server.

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

bd.com

Security Patches: BD Pyxis™ Supply

June 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for June 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
2023-06 Security Monthly Quality Rollup for Windows Server 2008 for x86-based Systems (KB5027279)	This cumulative security update contains improvements that are part of update KB5026408 (released May 9, 2023). This update also contains miscellaneous security improvements to internal Windows OS functionality. No specific issues are documented for this release. For more information about the resolved security vulnerabilities, please refer to the Deployments I Security Update Guide and the June 2023 Security Updates.	KB5027279	Applicable on Supply.
2023-06 Security Only Quality Update for Windows Server 2008 for x86-based Systems (KB5027277)	This update contains miscellaneous security improvements to internal Windows OS functionality. No additional issues were documented for this release. For more information about the resolved security vulnerabilities, please refer to the Deployments I Security Update Guide and the June 2023 Security Updates.	KB5027277	Applicable on Supply.
2023-06 Security and Quality Rollup for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7 (KB5027540)	CVE-2023-24897 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in the MSDIA SDK where corrupted PDBs can cause heap overflow, leading to a crash or remove code execution. For more information see CVE 2023-24897. CVE-2023-29326 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in WPF where the BAML offers other ways to instantiate types that leads to an elevation of privilege. For more information see CVE-2023-29326. CVE-2023-24895 - .NET Framework Remote Code Execution Vulnerability	KB5027540	Applicable on Supply.

	• This security update addresses a vulnerability in the WPF XAML parser where an unsandboxed parser can lead to remote code execution. For more information see CVE-2023-24895. CVE-2023-24936 - .NET Framework Elevation of Privilege Vulnerability • This security update addresses a vulnerability in bypass restrictions when deserializing a DataSet or DataTable from XML, leading to an elevation of privilege. For more information see CVE-2023-24936. CVE-2023-29331 - .NET Framework Denial of Service Vulnerability • This security update addresses a vulnerability where the AIA fetching process for client certificates can lead to denial of service. For more information see CVE 2023-29331. CVE-2023-32030 - .NET Framework Denial of Service Vulnerability • This security update addresses a vulnerability where X509Certificate2 file handling can lead to denial of service. For more information see CVE 2023-32030.		
2023-06 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems (KB5027275)	This cumulative security update contains improvements that are part of update KB5026413 (released May 9, 2023). This update also contains miscellaneous security improvements to internal Windows OS functionality. No specific issues are documented for this release. For more information about the resolved security vulnerabilities, please refer to the Deployments I Security Update Guide and the June 2023 Security Updates.	KB5027275	Applicable on Supply.
2023-06 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems (KB5027256)	This update contains miscellaneous security improvements to internal Windows OS functionality. No additional issues were documented for this release. For more information about the resolved security vulnerabilities, please refer to the Deployments I Security Update Guide and the June 2023 Security Updates.	KB5027256	Applicable on Supply.
2023-06 Security Only Update for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7 (KB5027531)	CVE-2023-24897 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in the MSDIA SDK where corrupted PDBs can cause heap overflow, leading to a crash or remove code execution. For more information see CVE 2023-24897. CVE-2023-29326 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in WPF where the BAML offers other ways to instantiate types that leads to an elevation of	KB5027531	Applicable on Supply.

	privilege. For more information see CVE-2023-29326. CVE-2023-24895 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in the WPF XAML parser where an unsandboxed parser can lead to remote code execution. For more information see CVE-2023-24895. CVE-2023-24936 - .NET Framework Elevation of Privilege Vulnerability • This security update addresses a vulnerability in bypass restrictions when deserializing a DataSet or DataTable from XML, leading to an elevation of privilege. For more information see CVE-2023-24936. CVE-2023-29331 - .NET Framework Denial of Service Vulnerability • This security update addresses a vulnerability where the AIA fetching process for client certificates can lead to denial of service. For more information see CVE 2023-29331. CVE-2023-32030 - .NET Framework Denial of Service Vulnerability • This security update addresses a vulnerability where X509Certificate2 file handling can lead to denial of service. For more information see CVE 2023-32030.		
2023-06 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 (KB5027542)	CVE-2023-24897 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in the MSDIA SDK where corrupted PDBs can cause heap overflow, leading to a crash or remove code execution. For more information see CVE 2023-24897. CVE-2023-29326 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in WPF where the BAML offers other ways to instantiate types that leads to an elevation of privilege. For more information see CVE-2023-29326. CVE-2023-24895 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in the WPF XAML parser where an unsandboxed parser can lead to remote code execution. For more information see CVE-2023-24895. CVE-2023-24936 - .NET Framework Elevation of Privilege Vulnerability • This security update addresses a vulnerability in bypass restrictions when deserializing a DataSet or DataTable from XML, leading to an elevation of privilege. For more information see CVE-2023-24936. CVE-2023-29331 - .NET Framework Denial of Service Vulnerability	KB5027542	Applicable on Supply.

	• This security update addresses a vulnerability where the AIA fetching process for client certificates can lead to denial of service. For more information see CVE 2023-29331. CVE-2023-32030 - .NET Framework Denial of Service Vulnerability • This security update addresses a vulnerability where X509Certificate2 file handling can lead to denial of service. For more information see CVE 2023-32030.		
2023-06 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5027271)	This cumulative security update includes improvements that are part of update KB5026415 (released May 9, 2023). This update also contains miscellaneous security improvements to internal Windows OS functionality. No specific issues are documented for this release. For more information about the resolved security vulnerabilities, please refer to the Deployments I Security Update Guide and the June 2023 Security Updates.	KB5027271	Applicable on Supply.
2023-06 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5027282)	This update contains miscellaneous security improvements to internal Windows OS functionality. No specific issues are documented for this release. For more information about the resolved security vulnerabilities, please refer to the Deployments I Security Update Guide and the June 2023 Security Updates.	KB5027282	Applicable on Supply.
2023-06 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 for x64 (KB5027533)	CVE-2023-24897 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in the MSDIA SDK where corrupted PDBs can cause heap overflow, leading to a crash or remove code execution. For more information see CVE 2023-24897. CVE-2023-29326 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in WPF where the BAML offers other ways to instantiate types that leads to an elevation of privilege. For more information see CVE-2023-29326. CVE-2023-24895 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in the WPF XAML parser where an unsandboxed parser can lead to remote code execution. For more information see CVE-2023-24895. CVE-2023-24936 - .NET Framework Elevation of Privilege Vulnerability • This security update addresses a vulnerability in bypass restrictions when deserializing a DataSet or DataTable from XML, leading to an elevation of privilege. For more information see CVE-2023-24936.	KB5027533	Applicable on Supply.

	CVE-2023-29331 - .NET Framework Denial of Service Vulnerability • This security update addresses a vulnerability where the AIA fetching process for client certificates can lead to denial of service. For more information see CVE 2023-29331. CVE-2023-32030 - .NET Framework Denial of Service Vulnerability • This security update addresses a vulnerability where X509Certificate2 file handling can lead to denial of service. For more information see CVE 2023-32030.		
2023-06 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5027219)	This security update includes quality improvements. When you install this KB: • This update addresses an issue that might cause a memory leak. The leak might occur during prolonged Remote Desktop audio redirection. • This update addresses an issue that affects the Windows Kernel. This issue is related to CVE-2023-32019. To learn more, see KB5028407.	KB5027219	Applicable on Supply.
2023-06 Cumulative Update for .NET Framework 4.8 for Windows Server 2016 for x64 (KB5027123)	CVE-2023-24897 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in the MSDIA SDK where corrupted PDBs can cause heap overflow, leading to a crash or remove code execution. For more information see CVE-2023-24897. CVE-2023-29326 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in WPF where the BAML offers other ways to instantiate types that leads to an elevation of privilege. For more information see CVE-2023-29326. CVE-2023-24895 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in the WPF XAML parser where an unsandboxed parser can lead to remote code execution. For more information see CVE-2023-24895. CVE-2023-24936 - .NET Framework Elevation of Privilege Vulnerability • This security update addresses a vulnerability in bypass restrictions when deserializing a DataSet or DataTable from XML, leading to an elevation of privilege. For more information see CVE-2023-24936. CVE-2023-29331 - .NET Framework Denial of Service Vulnerability • This security update addresses a vulnerability where the AIA fetching process for client certificates can lead to denial of service. For more information see CVE 2023-29331.	KB5027123	Applicable on Supply.

	CVE-2023-32030 - .NET Framework Denial of Service Vulnerability • This security update addresses a vulnerability where X509Certificate2 file handling can lead to denial of service. For more information see CVE-2023-32030.		
2023-06 Cumulative Update for Windows Server 2019 for x64-based Systems (KB5027222)	This security update includes improvements. When you install this KB: • This update addresses an issue that affects the Storage Spaces Direct (S2D) cluster. It might not come online. This occurs after a periodic password rollover. The error code is 1326. • This update addresses an issue that affects the Appx State Repository. When you remove a user profile, the cleanup is incomplete. Because of this, its database grows as time passes. This growth might cause delays when users sign in to multi-user environments like FSLogix. • This update addresses an issue that affects the Windows Remote Management (WinRM) client. The client returns an HTTP server error status (500). This error occurs when it runs a transfer job in thStorage Migration Service. • This update addresses an issue that affects signed Windows Defender Application Control (WDAC) policies. They are not applied to the Secure Kernel. This occurs when you enable Secure Boot. • This update addresses an issue that might affect the Local Security Authority Subsystem Service (LSASS). It might close sporadically. The system logs the exception 0xc0000710 in the Application Error event 1000. Because of this, the domain controller restarts unexpectedly. This issue affects read-only DCs (RODC) that also run Microsoft Defender Advanced Threat Protection (ATP). • This update addresses an issue that affects the Windows Kernel. This issue is related to CVE-2023-32019. To learn more, see KB5028407.	KB5027222	Applicable on Supply.
2023-06 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB5027222)	This security update includes improvements. When you install this KB: • This update addresses an issue that affects the Storage Spaces Direct (S2D) cluster. It might not come online. This occurs after a periodic password rollover. The error code is 1326. • This update addresses an issue that affects the Appx State Repository. When you remove a user profile, the cleanup is incomplete. Because of this, its database grows as time passes. This growth might cause delays when users sign in to multi-user environments like FSLogix. • This update addresses an issue that affects the Windows Remote Management (WinRM) client. The client returns an HTTP server error status	KB5027222	Applicable on Supply.

(500). This error occurs when it runs a transfer job in thStorage Migration Service.

- This update addresses an issue that affects signed Windows Defender Application Control (WDAC) policies. They are not applied to the Secure Kernel. This occurs when you enable Secure Boot.
- This update addresses an issue that might affect the Local Security Authority Subsystem Service (LSASS). It might close sporadically. The system logs the exception 0xc0000710 in the Application Error event 1000. Because of this, the domain controller restarts unexpectedly. This issue affects read-only DCs (RODC) that also run Microsoft Defender Advanced Threat Protection (ATP).
- This update addresses an issue that affects the Windows Kernel. This issue is related to CVE-2023-32019. To learn more, see KB5028407.

2023-06 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 (KB5027536)	CVE-2023-24897 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in the MSDIA SDK where corrupted PDBs can cause heap overflow, leading to a crash or remove code execution. For more information see CVE 2023-24897. CVE-2023-29326 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in WPF where the BAML offers other ways to instantiate types that leads to an elevation of privilege. For more information see CVE-2023-29326. CVE-2023-24895 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in the WPF XAML parser where an unsandboxed parser can lead to remote code execution. For more information see CVE-2023-24895. CVE-2023-24936 - .NET Framework Elevation of Privilege Vulnerability • This security update addresses a vulnerability in bypass restrictions when deserializing a DataSet or DataTable from XML, leading to an elevation of privilege. For more information see CVE-2023-24936. CVE-2023-29331 - .NET Framework Denial of Service Vulnerability • This security update addresses a vulnerability where the AIA fetching process for client certificates can lead to denial of service. For more information see CVE 2023-29331. CVE-2023-32030 - .NET Framework Denial of Service Vulnerability • This security update addresses a vulnerability where X509Certificate2 file handling can lead to denial of service. For more information see CVE 2023-32030.	**KB5027536**	Applicable on Supply.
2023-06 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10 Version 1809 for x64 (KB5027536)	CVE-2023-24897 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in the MSDIA SDK where corrupted PDBs can cause heap overflow, leading to a crash or remove code execution. For more information see CVE 2023-24897. CVE-2023-29326 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in WPF where the BAML offers other ways to instantiate types that leads to an elevation of privilege. For more information see CVE-2023-29326. CVE-2023-24895 - .NET Framework Remote Code Execution Vulnerability	KB5027536	Applicable on Supply.

	• This security update addresses a vulnerability in the WPF XAML parser where an unsandboxed parser can lead to remote code execution. For more information see CVE-2023-24895. CVE-2023-24936 - .NET Framework Elevation of Privilege Vulnerability • This security update addresses a vulnerability in bypass restrictions when deserializing a DataSet or DataTable from XML, leading to an elevation of privilege. For more information see CVE-2023-24936. CVE-2023-29331 - .NET Framework Denial of Service Vulnerability • This security update addresses a vulnerability where the AIA fetching process for client certificates can lead to denial of service. For more information see CVE 2023-29331. CVE-2023-32030 - .NET Framework Denial of Service Vulnerability • This security update addresses a vulnerability where X509Certificate2 file handling can lead to denial of service. For more information see CVE 2023-32030.		
Windows Malicious Software Removal Tool x64 - v5.114	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