Security Patches:
BD Pyxis™ Anesthesia System 3500

February 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for February 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
2023-02 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5022872 (released January 10, 2023). ▪ This update contains miscellaneous security improvements to internal Windows OS functionality. No specific issues are documented for this release.	KB5022872	Applicable on 3500/4000 Anesthesia System and MS3500/4000 Station
2023-02 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.	KB5022874	Applicable on 3500/4000 Anesthesia System and MS3500/4000 Station
2023-02 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems	This security update resolves vulnerabilities in Internet Explorer.	KB5022835	Applicable on 3500 and 4000 Anesthesia System

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

Security Patches:
BD Pyxis™ Anesthesia System 4000

February 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for February 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 - v5.110	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS 4000 Console and MS4000 Anesthesia and Station
2023-02 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	This update addresses security issues for your Windows operating system.	KB5022838	Applicable on MS4000 Anesthesia System and MS4000 Station
2023-02 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5022872 (released January 10, 2023). ▪ This update contains miscellaneous security improvements to internal Windows OS functionality. No specific issues are documented for this release.	KB5022872	Applicable on 3500/4000 Anesthesia System and MS3500/4000 Station
2023-02 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.	KB5022874	Applicable on 3500/4000 Anesthesia System and MS3500/4000 Station

2023-02 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems	This security update resolves vulnerabilities in Internet Explorer.	KB5022835	Applicable on 3500 and 4000 Anesthesia System

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

bd.com

Security Patches:
BD Pyxis™ MedStation™ 3500

February 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for February 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 - v5.110	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS3500 and MS4000 Console
2023-02 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5022872 (released January 10, 2023). This update contains miscellaneous security improvements to internal Windows OS functionality. No specific issues are documented for this release.	KB5022872	Applicable on 3500/4000 Anesthesia System and MS3500/4000 Station
2023-02 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.	KB5022874	Applicable on 3500/4000 Anesthesia System and MS3500/4000 Station
2023-02 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems	This security update resolves vulnerabilities in Internet Explorer.	KB5022835	Applicable on 3500 and 4000 Anesthesia System

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

bd.com

Security Patches:
BD Pyxis™ MedStation™ 4000

February 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for February 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 - v5.110	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS4000 Console and 4000 Anesthesia and Station
2023-02 Cumulative Update for Windows Server 2016 for x64-based Systems	This update addresses security issues for your Windows operating system.	KB5022838	Applicable on MS4000 Console
2023-02 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	This update addresses security issues for your Windows operating system.	KB5022838	Applicable on MS4000 Anesthesia System and MS4000 Station
2023-02 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5022872 (released January 10, 2023). ▪ This update contains miscellaneous security improvements to internal Windows OS functionality. No specific issues are documented for this release.	KB5022872	Applicable on 3500/4000 Anesthesia System and MS3500/4000 Station

2023-02 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.	KB5022874	Applicable on 3500/4000 Anesthesia System and MS3500/4000 Station
Windows Malicious Software Removal Tool x64 - v5.110	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS 4000 Console and MS4000 Anesthesia and Station
2023-02 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems	This security update resolves vulnerabilities in Internet Explorer.	KB5022835	Applicable on 3500 and 4000 Anesthesia System

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

bd.com

Security Patches: Security Module

February 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for February 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 - v5.109 (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.	KB890830	Applicable on Security Module devices
2023-02 Security and Quality Rollup for .NET Framework 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows Server 2012 R2 for x64 (KB5022513)	This update makes improvements for the following issues: - Addresses an issue in propagation of ElementHost controls Visible property to underlying HwndWrapper. - Addresses an issue that restores System.Windows.Controls.VirtualizingStackPanel scrolling behavior for CollectionChange event.	KB5022513	Applicable on Security Module devices.
2023-02 Security Only Update for .NET Framework 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows Server 2012 R2 for x64 (KB5022524)	CVE-2023-21808 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in the MSDIA SDK where an untrusted pointer dereference can cause memory corruption, leading to a crash or remove code execution. For more information please see CVE-2023-21808.	KB5022524	Applicable on Security Module devices.
2023-02 Security and Quality Rollup for .NET Framework 3.5 for Windows Server 2012 R2 for x64 (KB5022525)	CVE-2023-21722 - .NET Framework Denial of Service Vulnerability This security update addresses a vulnerability where the Visual Studio WMI Setup Provider Installer can be used by a low level, local attacker to corrupt local files that SYSTEM can writ to, leading to a potential denial of service. For more information please see CVE-2023-21722.	KB5022525	Applicable on Security Module devices.

2023-02 Security Only Update for .NET Framework 3.5 for Windows Server 2012 R2 for x64 (KB5022531)	CVE-2023-21722 - .NET Framework Denial of Service Vulnerability This security update addresses a vulnerability where the Visual Studio WMI Setup Provider Installer can be used by a low level, local attacker to corrupt local files that SYSTEM can writ to, leading to a potential denial of service. For more information please see CVE-2023-21722.	KB5022531	Applicable on Security Module devices.
2023-02 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems (KB5022835)	• The improvements that are included in this update are also included in the February 2023 Security Monthly Quality Rollup. Installing either this update or the Security Monthly Quality Rollup installs the same improvements. • This update is not applicable for installation on a device on which the Security Monthly Quality Rollup from February 2023 (or a later month) is already installed. This is because that update contains all the same improvements that are included in this update.	KB5022835	Applicable on Security Module devices.
2023-02 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5022894)	This update contains miscellaneous security improvements to internal Windows OS functionality. No specific issues are documented for this release.	KB5022894	Applicable on Security Module devices.
2023-02 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5022899)	This cumulative security update includes improvements that are part of update KB5022352 (released January 10, 2023). • This update contains miscellaneous security improvements to internal Windows OS functionality. No specific issues are documented for this release.	KB5022899	Applicable on Security Module devices.
2023-02 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 (KB5022733)	CVE-2023-21808 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in the MSDIA SDK where an untrusted pointer dereference can cause memory corruption, leading to a crash or remove code execution. For more information please see CVE-2023-21808.	KB5022733	Applicable on Security Module devices.
2023-02 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 (KB5022785)	CVE-2023-21808 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in the MSDIA SDK where an untrusted pointer dereference can cause memory corruption, leading to a crash or remove code execution. For more information please see CVE-2023-21808.	KB5022785	Applicable on Security Module devices.

2023-02 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5022838)	This security update includes quality improvements. When you install this KB: • This update addresses an issue that puts domain controllers (DC) in a restart loop. This occurs because the Local Security Authority Subsystem Service (LSASS) stops responding. The error is 0xc0000374. LSASS stops responding if you populate KrbTGT with the AltsecID on accounts that read-write and read-only DCs use. This update addresses an issue that affects AppV. It stops file names from having the correct letter case (uppercase or lowercase).	KB5022838	Applicable on Security Module devices.

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

bd.com

Security Patches: BD Pyxis™ IV Prep

February 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for February 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 - v5.109	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
2023-02 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.	KB5022838	Applicable on Cato

2023-02 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.	KB5022733	Applicable on Cato
2023-02 Cumulative Security Update for Internet Explorer 11 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	KB5022835	Applicable on Cato
2023-02 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	KB5022894	Applicable on Cato
2023-02 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	KB5022899	Applicable on Cato

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

bd.com

Security Patches: BD Pyxis Connect

February 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for February 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
2023-02 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5022899)	This update contains miscellaneous security improvements to internal Windows OS functionality. No specific issues are documented for this release.	KB5022899	N/A
2023-02 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems (KB5022835)	This security update resolves vulnerabilities in Internet Explorer. This update applies to the following: • Internet Explorer 11 on Windows Server 2012 R2 • Internet Explorer 11 on Windows Server 2012 • Internet Explorer 11 on Windows Server 2008 R2 SP1 • Internet Explorer 9 on Windows Server 2008 SP2	KB5022835	N/A
Windows Malicious Software Removal Tool x64 - v5.110 (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

2023-02 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 (KB5022733)	This is a cumulative Update for 3.5, 4.8 and 4.8.1 for Windows 11, version 21H2.	KB5022733	N/A
2023-02 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 (KB5022785)	This security update addresses the following: • Vulnerability in the MSDIA SDK where an untrusted pointer dereference can cause memory corruption, leading to a crash or remove code execution. • Vulnerability where the Visual Studio WMI Setup Provider Installer can be used by a low level, local attacker to corrupt local files that SYSTEM can writ to, leading to a potential denial of service.	KB5022785	N/A
2023-02 Cumulative Update for .NET Framework 4.8 for Windows Server 2016 for x64 (KB5022503)	This update is for Windows 10, version 1607 and Windows Server 2016 includes cumulative reliability improvements in .NET Framework 4.8.	KB5022503	N/A
2023-02 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2 for x64 (KB5022729)	This is a cumulative update for 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2. It addresses the following security improvements: • .NET Framework Remote Code Execution Vulnerability: This security update addresses a vulnerability in the MSDIA SDK where an untrusted pointer dereference can cause memory corruption, leading to a crash or remove code execution. • .NET Framework Denial of Service Vulnerability: This security update addresses a vulnerability where the Visual Studio WMI Setup Provider Installer can be used by a low level, local attacker to corrupt local files that SYSTEM can writ to, leading to a potential denial of service.	KB5022729	N/A
2023-02 Cumulative Update Preview for Windows 10 Version 22H2 for x64-based Systems (KB5022906)	This update includes the following: • Addresses an issue that affects IE mode. The text on the status bar is not always visible. • Addresses accessibility issues. They affect Narrator on the Settings home page. • Addresses an issue that stops hyperlinks from working in Microsoft Excel. • Addresses an issue that affects a certain streaming app. The issue stops video playback after an advertisement plays in the app.	KB5022906	N/A

2023-02 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5022838)	This update includes the following: • Addresses a key issue that puts domain controllers (DC) in a restart loop. This problem usually occurs because the Local Security Authority Subsystem Service (LSASS) stops responding, and results in an error 0xc0000374. • After installing this update, administrators can now reset the zoom for HTML dialogs to the default. This update will affect HTML dialogs in Microsoft Edge IE mode. • Resolves an issue affecting AppV. Previously, it used to stop file names from having the correct letter case (uppercase or lowercase). • Works on a known issue affecting certain Internet of Things (IoT) devices in which they lose audio. • Addresses a key issue affecting the searchindexer.exe which randomly stops you from signing in or signing out.	KB5022838	N/A

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

bd.com

Security Patches: BD Pharmogistics

February 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for February 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.

2023-02 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems	This cumulative security update includes improvements that are part of update KB5022352 (released January 10, 2023). 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 | Security Update Guide and the February 2023 Security Updates.	KB5022899	N/A
2023-02 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	Security Improvements CVE-2023-21808 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in the MSDIA SDK where an untrusted pointer dereference can cause memory corruption, leading to a crash or remove code execution. For more information please see CVE-2023-21808. CVE-2023-21722 - .NET Framework Denial of Service Vulnerability This security update addresses a vulnerability where the Visual Studio WMI Setup Provider Installer can be used by a low level, local attacker to corrupt local files that SYSTEM can writ to, leading to a potential denial of service. For more information please see CVE-2023-21722.	KB5022733	N/A
2023-02 Cumulative Update for Windows 10 Version 22H2 for x64-based Systems	Windows 10 servicing stack update - 19042.2300, 19044.2300, and 19045.2300 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.	KB5022834	N/A

2023-02 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 21H2 for x64	Security Improvements CVE-2023-21808 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in the MSDIA SDK where an untrusted pointer dereference can cause memory corruption, leading to a crash or remove code execution. For more information please see CVE-2023-21808. CVE-2023-21722 - .NET Framework Denial of Service Vulnerability This security update addresses a vulnerability where the Visual Studio WMI Setup Provider Installer can be used by a low level, local attacker to corrupt local files that SYSTEM can writ to, leading to a potential denial of service. For more information please see CVE-2023-21722.	KB5022728	N/A
for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.2301.6)	Microsoft Defender Antivirus requires monthly updates (KB4052623) known as platform updates. You can manage the distribution of updates through one of the following methods: Windows Server Update Service (WSUS) Microsoft Configuration Manager The usual methods you use to deploy Microsoft and Windows updates to endpoints in your network.	KB4052623	N/A

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

Security Patches: PARx

Feb 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for Feb 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 - v5.110	Windows Malicious Software Removal Tool (MSRT) 5.83 helps remove malicious software from computers running Windows 10, Windows 8.1, Windows Server 2012 R2, Windows 8, Windows Server 2012, Windows 7, or Windows Server 2008.	KB890830	Applicable on ParX
2023-02 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	Windows 10 version 1607 with this security update – • Addresses a key issue that puts domain controllers (DC) in a restart loop. This problem usually occurs because the Local Security Authority Subsystem Service (LSASS) stops responding, and results in an error 0xc0000374. • After installing this update, administrators can now reset the zoom for HTML dialogs to the default. This update will affect HTML dialogs in Microsoft Edge IE mode. • Resolves an issue affecting AppV. Previously, it used to stop file names from having the correct letter case (uppercase or lowercase). • Works on a known issue affecting certain Internet of Things (IoT) devices in which they lose audio.	KB5022838	Applicable on ParX

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

bd.com

Security Patches: TIM

Feb 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for Feb 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 - v5.110	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. 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	KB890830	Applicable on TIM.

2023-02 Cumulative Update for .NET Framework 4.8 for Windows Server 2016 for x64	release information. It also includes information for the administrators and advanced users, including information about supported command-line switches. CVE-2023-21808 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in the MSDIA SDK where an untrusted pointer dereference can cause memory corruption, leading to a crash or remove code execution. For more information please see CVE-2023-21808.	KB5022503	Applicable on TIM.
2023-02 Cumulative Update for Windows Server 2016 for x64-based Systems	CVE-2023-21722 - .NET Framework Denial of Service Vulnerability This security update addresses a vulnerability where the Visual Studio WMI Setup Provider Installer can be used by a low level, local attacker to corrupt local files that SYSTEM can writ to, leading to a potential denial of service. For more information please see CVE-2023-21722. This security update includes quality improvements. When you install this KB: This update addresses an issue that puts domain controllers (DC) in a restart loop. This occurs because the Local Security Authority Subsystem Service (LSASS) stops responding. The error is 0xc0000374. LSASS stops responding if you populate KrbTGT with the AltsecID on accounts that read-write and read-only DCs use. This update affects HTML dialogs in Microsoft Edge IE mode. Administrators can now reset the zoom for HTML dialogs to the default. This update addresses an issue that affects AppV. It stops file names from having the correct letter case (uppercase or lowercase).	KB5022838	Applicable on TIM.
2023-02 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 update addresses an issue that affects certain Internet of Things (IoT) devices. They lose audio. This update addresses an issue that affects searchindexer.exe. It randomly stops you from signing in or signing out. If you installed earlier updates, only the new updates contained in this package will be downloaded and installed on your device.	KB5022733	Applicable on TIM.

For more information about security vulnerabilities, please refer to the new Security Update Guide website and the February 2023 Security Updates

CVE-2023-21808 - .NET Framework Remote Code Execution Vulnerability

This security update addresses a vulnerability in the MSDIA SDK where an untrusted pointer dereference can cause memory corruption, leading to a crash or remove code execution. For more information please see CVE-2023-21808.

CVE-2023-21722 - .NET Framework Denial of Service Vulnerability

This security update addresses a vulnerability where the Visual Studio WMI Setup Provider Installer can be used by a low level, local attacker to corrupt local files that SYSTEM can writ to, leading to a potential denial of service. For more information please see CVE-2023-21722.

2023-02 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems	This security update resolves vulnerabilities in Internet Explorer. To learn more about these vulnerabilities, see Deployments | Security Update Guide. Additionally, see the following articles for more information about cumulative updates: Windows Server 2008 SP2 update history Windows 7 SP1 and Windows Server 2008 R2 SP1 update history Windows Server 2012 update history Windows 8.1 and Windows Server 2012 R2 update history	KB5022835	Applicable on TIM.
2023-02 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 | Security Update Guide and the February 2023 Security Updates.	KB5022894	Applicable on TIM.
2023-02 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-2023-21808 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in the MSDIA SDK where an untrusted pointer dereference can cause memory corruption, leading to a crash or remove code execution. For more information please see CVE-2023-21808. CVE-2023-21722 - .NET Framework Denial of Service Vulnerability This security update addresses a vulnerability where the Visual Studio WMI Setup Provider Installer can be used by a low level, local attacker to corrupt local files that SYSTEM can writ to, leading to a potential denial of service. For more information please see CVE-2023-21722.	KB5022785	Applicable on TIM.

2023-02 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems	This cumulative security update includes improvements that are part of update KB5022352 (released January 10, 2023). 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 | Security Update Guide and the February 2023 Security Updates.	KB5022899	Applicable on TIM.

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

bd.com

Security Patches:
BD **Pyxis™ Anesthesia ES**

February 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for February 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
2023-02 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.	KB5022840	Applicable on 1.7.1,1.7.2,1.7.3 PAS device.
2023-02 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.	KB5022782	Applicable on 1.7.1,1.7.2,1.7.3 PAS device..

2023-02 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.	KB5022834	Applicable on 1.7.1,1.7.2,1.7.3 PAS device.
2023-02 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.	KB5022728	Applicable on 1.7.1,1.7.2,1.7.3 PAS device.
Windows Malicious Software Removal Tool x64 - v5.110	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 PAS device.

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

bd.com

Security Patches:
BD **Pyxis™ Anesthesia ES**

February 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for February 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
2023-02 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.	KB5022874	Applicable on PAS device.
2023-02 Cumulative Security Update for Internet Explorer 11 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.	KB5022835	Applicable on PAS device.

Windows Malicious Software Removal Tool x64 - v5.110	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.
2023-02 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.	KB5022872	Applicable on PAS device.
2023-02 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.	KB5022838	Applicable on PAS device.

2023-02 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.	KB5022840	Applicable on PAS device.
2023-02 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.	KB5022782	Applicable on PAS device.

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

bd.com

Security Patches: BD Pyxis™ CIISafe ES

February 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for February 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
2023-02 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.	KB5022840	Applicable on CIISafe device.
2023-02 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.	KB5022782	Applicable on CIISafe device.

2023-02 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.	KB5022834	Applicable on CIISafe device.
2023-02 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.	KB5022728	Applicable on CIISafe device.
Windows Malicious Software Removal Tool x64 - v5.110	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**

February 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for February 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
2023-02 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.	KB5022840	Applicable on 1.7.1,1.7.2,1.7.3 MedSTN device.
2023-02 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.	KB5022782	Applicable on 1.7.1,1.7.2,1.7.3 MedSTN device.

2023-02 Cumulative Update Preview 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.	KB5022906	Applicable on 1.7.1,1.7.2,1.7.3 MedSTN device.
2023-02 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.	KB5022728	Applicable on 1.7.1,1.7.2,1.7.3 MedSTN device.
Windows Malicious Software Removal Tool x64 - v5.110	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™ Medstation ES**

February 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for February 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
2023-02 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.	KB5022872	Applicable on Medstn ES device.
2023-02 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.	KB5022874	Applicable on Medstn ES device.

Windows Malicious Software Removal Tool x64 - v5.110	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.
2023-02 Cumulative Security Update for Internet Explorer 11 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.	KB5022835	Applicable on Medstn ES device.
2023-02 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.	KB5022838	Applicable on Medstn ES device.

2023-02 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.	KB5022503	Applicable on Medstn ES device.
2023-02 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.	KB5022840	Applicable on Medstn device.
2023-02 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.	KB5022782	Applicable on Medstn device.

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

bd.com

Security Patches:
BD **Pyxis™ ES Server**

February 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for February 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
2023-02 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.	KB5022840	Applicable on ES 1.7.1,1.7.2,1.7.3 Server.
2023-02 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.	KB5022782	Applicable on ES 1.7.1,1.7.2,1.7.3 Server.

Windows Malicious Software Removal Tool x64 - v5.110	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 ES 1.7.1,1.7.2,1.7.3 Server.

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

bd.com

Security Patches:
BD **Pyxis™ MedES Server**

February 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for February 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
2023-02 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.	KB5022899	Applicable on MedES Server.
2023-02 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.	KB5022785	Applicable on MedES Server.

2023-02 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.	KB5022894	Applicable on MedES Server.
2023-02 Cumulative Security Update for Internet Explorer 11 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.	KB5022835	Applicable on MedES Server.
2023-02 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.	KB5022733	Applicable on MedES Server.

2023-02 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.	KB5022838	Applicable on MedES Server.
Windows Malicious Software Removal Tool x64 - v5.110	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.

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

bd.com

Security Patches: BD Pyxis™ Supply

February 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for February 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
2023-02 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems (KB5022835)	This security update resolves vulnerabilities in Internet Explorer. To learn more about these vulnerabilities, see Deployments | Security Update Guide.	KB5022835	Applicable on Supply.
2023-02 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 (KB5022733)	CVE-2023-21808 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in the MSDIA SDK where an untrusted pointer dereference can cause memory corruption, leading to a crash or remove code execution. For more information please see CVE-2023-21808. CVE-2023-21722 - .NET Framework Denial of Service Vulnerability This security update addresses a vulnerability where the Visual Studio WMI Setup Provider Installer can be used by a low level, local attacker to corrupt local files that SYSTEM can writ to, leading to a potential denial of service. For more information please see CVE-2023-21722.	KB5022733	Applicable on Supply.

2023-02 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5022899)	This cumulative security update includes improvements that are part of update KB5022352 (released January 10, 2023). • This update contains miscellaneous security improvements to internal Windows OS functionality. No specific issues are documented for this release.	KB5022899	Applicable on Supply.
2023-02 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5022894)	This update contains miscellaneous security improvements to internal Windows OS functionality. No specific issues are documented for this release.	KB5022894	Applicable on Supply.
2023-02 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 (KB5022785) 2023-01 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5022352)	CVE-2023-21808 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in the MSDIA SDK where an untrusted pointer dereference can cause memory corruption, leading to a crash or remove code execution. For more information please see CVE-2023-21808. CVE-2023-21722 - .NET Framework Denial of Service Vulnerability This security update addresses a vulnerability where the Visual Studio WMI Setup Provider Installer can be used by a low level, local attacker to corrupt local files that SYSTEM can writ to, leading to a potential denial of service. For more information please see CVE-2023-21722.	KB5022785	Applicable on Supply.
2023-02 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems (KB5022872)	This cumulative security update contains improvements that are part of update KB5022872 (released January 10, 2023). • This update contains miscellaneous security improvements to internal Windows OS functionality. No specific issues are documented for this release.	KB5022872	Applicable on Supply.
2023-02 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems (KB5022874)	This update contains miscellaneous security improvements to internal Windows OS functionality. No additional issues were documented for this release.	KB5022874	Applicable on Supply.

2023-02 Cumulative Update for .NET Framework 4.8 for Windows Server 2016 for x64 (KB5022503)	CVE-2023-21808 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in the MSDIA SDK where an untrusted pointer dereference can cause memory corruption, leading to a crash or remove code execution. For more information please see CVE-2023-21808. CVE-2023-21722 - .NET Framework Denial of Service Vulnerability This security update addresses a vulnerability where the Visual Studio WMI Setup Provider Installer can be used by a low level, local attacker to corrupt local files that SYSTEM can writ to, leading to a potential denial of service. For more information please see CVE-2023-21722.	KB5022503	Applicable on Supply.
2023-02 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5022838)	This security update includes quality improvements. When you install this KB: • This update addresses an issue that puts domain controllers (DC) in a restart loop. This occurs because the Local Security Authority Subsystem Service (LSASS) stops responding. The error is 0xc0000374. LSASS stops responding if you populate KrbTGT with the AltsecID on accounts that read-write and read-only DCs use. • This update addresses an issue that affects AppV. It stops file names from having the correct letter case (uppercase or lowercase). • This update addresses an issue that affects certain Internet of Things (IoT) devices. They lose audio. • This update addresses an issue that affects searchindexer.exe. It randomly stops you from signing in or signing out.	KB5022838	Applicable on Supply.

2023-02 Cumulative Update for Windows Server 2019 for x64-based Systems (KB5022840)	This security update includes improvements. When you install this KB: • New! It updates the text and web link for Windows Admin Center (WAC) notifications. These appear after you sign in to the desktop unless you have turned them off. The WAC notifications highlight the available Windows Server management options. • This update addresses an issue that affects searchindexer.exe. It randomly stops you from signing in or signing out. • This update addresses an issue that affects certain Internet of Things (IoT) devices. They lose audio. • This update addresses an issue that affects local Kerberos authentication. It fails if the local Key Distribution Center (KDC) service is not active. • This update addresses an issue that affects Windows Server 2022. Phone activation of a Key Management Services (KMS) key does not work. • This update affects Active Directory (AD). It improves the replication performance of AD in large environments. • This update addresses an issue that affects the Resilient File System (ReFS) MSba tag. The issue causes a nonpaged pool leak. • This update addresses an issue that affects the Resilient File System (ReFS). The issue causes high nonpaged pool usage, which depletes system memory.	KB5022840	Applicable on Supply.

2023-02 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB5022840)	This security update includes improvements. When you install this KB: • New! It updates the text and web link for Windows Admin Center (WAC) notifications. These appear after you sign in to the desktop unless you have turned them off. The WAC notifications highlight the available Windows Server management options. • This update addresses an issue that affects searchindexer.exe. It randomly stops you from signing in or signing out. • This update addresses an issue that affects certain Internet of Things (IoT) devices. They lose audio. • This update addresses an issue that affects local Kerberos authentication. It fails if the local Key Distribution Center (KDC) service is not active. • This update addresses an issue that affects Windows Server 2022. Phone activation of a Key Management Services (KMS) key does not work. • This update affects Active Directory (AD). It improves the replication performance of AD in large environments. • This update addresses an issue that affects the Resilient File System (ReFS) MSba tag. The issue causes a nonpaged pool leak. • This update addresses an issue that affects the Resilient File System (ReFS). The issue causes high nonpaged pool usage, which depletes system memory.	KB5022840	Applicable on Supply.

2023-02 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 (KB5022782)	• CVE-2023-21808 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in the MSDIA SDK where an untrusted pointer dereference can cause memory corruption, leading to a crash or remove code execution. For more information please see CVE-2023-21808. • CVE-2023-21722 - .NET Framework Denial of Service Vulnerability This security update addresses a vulnerability where the Visual Studio WMI Setup Provider Installer can be used by a low level, local attacker to corrupt local files that SYSTEM can writ to, leading to a potential denial of service. For more information please see CVE-2023-21722.	KB5022782	Applicable on Supply.

2023-02 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10 Version 1809 for x64 (KB5022782)	• CVE-2023-21808 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in the MSDIA SDK where an untrusted pointer dereference can cause memory corruption, leading to a crash or remove code execution. For more information please see CVE-2023-21808. • CVE-2023-21722 - .NET Framework Denial of Service Vulnerability This security update addresses a vulnerability where the Visual Studio WMI Setup Provider Installer can be used by a low level, local attacker to corrupt local files that SYSTEM can writ to, leading to a potential denial of service. For more information please see CVE-2023-21722.	KB5022782	**Applicable on Supply.**
Windows Malicious Software Removal Tool x64 - v5.109	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.

2023-02 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 1809 for x64 (KB5022504)	• CVE-2023-21808 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in the MSDIA SDK where an untrusted pointer dereference can cause memory corruption, leading to a crash or remove code execution. For more information please see CVE-2023-21808. • CVE-2023-21722 - .NET Framework Denial of Service Vulnerability This security update addresses a vulnerability where the Visual Studio WMI Setup Provider Installer can be used by a low level, local attacker to corrupt local files that SYSTEM can writ to, leading to a potential denial of service. For more information please see CVE-2023-21722.	KB5022504	Applicable on Supply.
2023-02 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows Server 2019 for x64 (KB5022504)	• CVE-2023-21808 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in the MSDIA SDK where an untrusted pointer dereference can cause memory corruption, leading to a crash or remove code execution. For more information please see CVE-2023-21808. • CVE-2023-21722 - .NET Framework Denial of Service Vulnerability This security update addresses a vulnerability where the Visual Studio WMI Setup Provider Installer can be used by a low level, local attacker to corrupt local files that SYSTEM can writ to, leading to a potential denial of service. For more information please see CVE-2023-21722.	KB5022504	Applicable on Supply.

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

bd.com