Security Patches:
BD Pyxis™ Anesthesia System 3500

May 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for May 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

Customers that maintain patches independent of BD automated delivery should ensure the validated patches are installed on their BD systems as the acting responsible entity in order to maintain the correct security posture of the system(s).

Microsoft® patches

Patch name	Description	Patch ID	Notes
2022-05 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems.	This cumulative security update contains improvements that are part of update KB5012626 (released April 12, 2022) and includes new improvements for the following issues:The Key Distribution Center (KDC) code incorrectly returns error message KDC_ERR_TGT_REVOKED during Domain Controller shutdown.After installing the January 2022 Windows update or a later Windows update on the Primary Domain Controller emulator (PDCe), listing or modifying name suffixes routing by using Netdom.exe or "Active Directory Domains and Trusts" snap-in may fail and you receive the following error message: "Insufficient system resources exist to complete the requested service."The Primary Domain Controller (PDC) for the root domain incorrectly logs warning and error events in the System log when trying to scan outbound-only trusts.	KB5014012	Applicable on 3500 Anesthesia System and MS3500 Station

2022-05 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	Security Improvements: This security update addresses an issue where a local user opening a specially crafted file could cause a denial-of-service condition on an affected system. For more information, please see CVE-2022-30130. Quality Improvements: For a list of improvements that were released with this update, please see the article links in the Additional Information section of this article.	KB5013870	Applicable on 3500 Anesthesia System and MS3500 Station
2022-05 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 an issue where a local user opening a specially crafted file could cause a denial of service condition on an affected system.	KB5013837	Applicable on 3500 Anesthesia System and MS3500 Station
2022-05 Security Only Quality Update for Windows 7 for x86-based Systems.	This security-only update includes new improvements for the following issues:The Key Distribution Center (KDC) code incorrectly returns error message KDC_ERR_TGT_REVOKED during Domain Controller shutdown.The Primary Domain Controller (PDC) for the root domain incorrectly logs warning and error events in the System log when trying to scan outbound-only trusts.	KB5013999	Applicable on 3500 Anesthesia System and MS3500 Station

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

bd.com

Security Patches:
BD Pyxis™ Anesthesia System 4000

May 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for May 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

Customers that maintain patches independent of BD automated delivery should ensure the validated patches are installed on their BD systems as the acting responsible entity in order to maintain the correct security posture of the system(s).

Microsoft® patches

Patch name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.101	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS4000 Console, Anesthesia System and Station
2022-05 Servicing Stack Update for Windows 10 Version 1607 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. Additionally, this update adds improvements for servicing the Secure Boot component of Windows.	KB5014026	Applicable on Anesthesia System and MS4000
2022-05 Cumulative Update for Windows 10 Version 1607 for x64-based Systems.	This security update includes quality improvements. Key changes include: New! Adds improvements for servicing the Secure Boot component of Windows. Addresses an issue that might occur when you use Netdom.exe or the Active Directory Domains and Trusts snap-in to list or modify name suffixes routing. These procedures might fail. The error message is, "Insufficient system resources exist to complete the requested service." This issue occurs after installing the January 2022 security update on the primary domain controller emulator (PDCe). Addresses an issue that causes the improper cleanup of Dynamic Data Exchange (DDE) objects. This prevents session teardown and causes a session to stop responding. Addresses an issue that might cause Kerberos.dll to stop working within the Local Security Authority Subsystem Service (LSASS). This occurs when LSASS processes simultaneous Service for User (S4U)	KB5013952	Applicable on Anesthesia System and MS4000

	user-to-user (U2U) requests for the same client user. Addresses a known issue that might prevent recovery discs (CD or DVD) from starting if you created them using the Backup and Restore (Windows 7) app in Control Panel. This issue occurs after installing Windows updates released January 11, 2022 or later.		
2022-05 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems.	This cumulative security update contains improvements that are part of update KB5012626 (released April 12, 2022) and includes new improvements for the following issues: The Key Distribution Center (KDC) code incorrectly returns error message KDC_ERR_TGT_REVOKED during Domain Controller shutdown. After installing the January 2022 Windows update or a later Windows update on the Primary Domain Controller emulator (PDCe), listing or modifying name suffixes routing by using Netdom.exe or "Active Directory Domains and Trusts" snap-in may fail and you receive the following error message: "Insufficient system resources exist to complete the requested service." The Primary Domain Controller (PDC) for the root domain incorrectly logs warning and error events in the System log when trying to scan outbound-only trusts.	KB5014012	Applicable on Anesthesia System and Station
2022-05 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.	Security Improvements: This security update addresses an issue where a local user opening a specially crafted file could cause a denial of service condition on an affected system. For more information please see CVE-2022-30130.Quality Improvements: For a list of improvements that were released with this update, please see the article links in the Additional Information section of this article.	KB5013870	Applicable on Anesthesia System and Station
2022-05 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 an issue where a local user opening a specially crafted file could cause a denial of service condition on an affected system.	KB5013837	Applicable on Anesthesia System and Station
2022-05 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems.	This security-only update includes new improvements for the following issues: The Key Distribution Center (KDC) code incorrectly returns error message KDC_ERR_TGT_REVOKED during Domain Controller shutdown. The Primary Domain Controller (PDC) for the root domain incorrectly logs warning and error events in the System log when trying to scan outbound-only trusts.	KB5013999	Applicable on Anesthesia System and Station

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

bd.com

Security Patches:
BD Pyxis™ MedStation™ 3500

May 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for May 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

Customers that maintain patches independent of BD automated delivery should ensure the validated patches are installed on their BD systems as the acting responsible entity in order to maintain the correct security posture of the system(s).

Microsoft® patches

Patch name	Description	Patch ID	Notes
2022-05 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems.	This cumulative security update contains improvements that are part of update KB5012626 (released April 12, 2022) and includes new improvements for the following issues: The Key Distribution Center (KDC) code incorrectly returns error message KDC_ERR_TGT_REVOKED during Domain Controller shutdown. After installing the January 2022 Windows update or a later Windows update on the Primary Domain Controller emulator (PDCe), listing or modifying name suffixes routing by using Netdom.exe or "Active Directory Domains and Trusts" snap-in may fail and you receive the following error message: "Insufficient system resources exist to complete the requested service." The Primary Domain Controller (PDC) for the root domain incorrectly logs warning and error events in the System log when trying to scan outbound-only trusts.	KB5014012	Applicable on MS3500 Station, MS3500 Anesthesia System and Med4000 windows 7.
2022-05 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	Security Improvements: This security update addresses an issue where a local user opening a specially crafted file could cause a denial of service condition on an affected system. For more information please see CVE-2022-30130. Quality Improvements: For a list of improvements that were released with this update, please see the article links in the Additional Information section of this article.	KB5013870	Applicable on MS3500 Station, MS3500 Anesthesia System and Med4000 windows 7.

2022-05 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 an issue where a local user opening a specially crafted file could cause a denial of service condition on an affected system.	KB5013837	Applicable on MS3500 Station, MS3500 Anesthesia System and Med4000 windows 7.
2022-05 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This security-only update includes new improvements for the following issues: The Key Distribution Center (KDC) code incorrectly returns error message KDC_ERR_TGT_REVOKED during Domain Controller shutdown. The Primary Domain Controller (PDC) for the root domain incorrectly logs warning and error events in the System log when trying to scan outbound-only trusts.	KB5013999	Applicable on MS3500 Station, MS3500 Anesthesia System and Med4000 windows 7.
2022-05 Security Only Quality Update for Windows Server 2008 for x86-based Systems.	This security-only update includes new improvements for the following issues: The Key Distribution Center (KDC) code incorrectly returns error message KDC_ERR_TGT_REVOKED during Domain Controller shutdown. The Primary Domain Controller (PDC) for the root domain incorrectly logs warning and error events in the System log when trying to scan outbound-only trusts.	KB5014006	Applicable on MS3500 and MS 4000 Console
2022-05 Security Monthly Quality Rollup for Windows Server 2008 for x86-based Systems.	This cumulative security update contains improvements that are part of update KB5012658 (released April 12, 2022) and includes new improvements for the following issues:The Key Distribution Center (KDC) code incorrectly returns error message KDC_ERR_TGT_REVOKED during Domain Controller shutdown. After installing the January 2022 Windows update or a later Windows update on the Primary Domain Controller emulator (PDCe), listing or modifying name suffixes routing by using Netdom.exe or "Active Directory Domains and Trusts" snap-in may fail and you receive the following error message: "Insufficient system resources exist to complete the requested service. "The Primary Domain Controller (PDC) for the root domain incorrectly logs warning and error events in the System log when trying to scan outbound-only trusts.	KB5014010	Applicable on MS3500 and MS 4000 Console
Windows Malicious Software Removal Tool - v5.101	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS3500 and MS 4000 Console

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

bd.com

Security Patches: BD Pyxis™ MedStation™ 4000

May 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for May 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

Customers that maintain patches independent of BD automated delivery should ensure the validated patches are installed on their BD systems as the acting responsible entity in order to maintain the correct security posture of the system(s).

Microsoft® patches

Patch name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.101	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS4000 Console, Anesthesia System and Station
2022-05 Servicing Stack Update for Windows Server 2016 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.	KB5014026	Applicable on MS4000 Console
2022-05 Cumulative Update for Windows Server 2016 for x64-based Systems.	This security update includes quality improvements. Key changes include: New! Adds improvements for servicing the Secure Boot component of Windows. Addresses an issue that might occur when you use Netdom.exe or the Active Directory Domains and Trusts snap-in to list or modify name suffixes routing. These procedures might fail. The error message is, "Insufficient system resources exist to complete the requested service." This issue occurs after installing the January 2022 security update on the primary domain controller emulator (PDCe). Addresses an issue that causes the improper cleanup of Dynamic Data Exchange (DDE) objects. This prevents session teardown and causes a session to stop responding. Addresses an issue that might cause Kerberos.dll to stop working within the Local Security Authority Subsystem Service (LSASS). This occurs when LSASS processes simultaneous Service for User (S4U) user-to-user (U2U) requests for the same client user. Addresses a known issue that might prevent recovery discs (CD or DVD) from starting if you created them using the Backup and Restore (Windows	KB5013952	Applicable on MS4000 Console

	7) app in Control Panel. This issue occurs after installing Windows updates released January 11, 2022 or later.		
2022-05 Servicing Stack Update for Windows 10 Version 1607 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.	KB5014026	Applicable on MS4000 and Anesthesia System
2022-05 Cumulative Update for Windows 10 Version 1607 for x64-based Systems.	This security update includes quality improvements. Key changes include: New! Adds improvements for servicing the Secure Boot component of Windows. Addresses an issue that might occur when you use Netdom.exe or the Active Directory Domains and Trusts snap-in to list or modify name suffixes routing. These procedures might fail. The error message is, "Insufficient system resources exist to complete the requested service." This issue occurs after installing the January 2022 security update on the primary domain controller emulator (PDCe). Addresses an issue that causes the improper cleanup of Dynamic Data Exchange (DDE) objects. This prevents session teardown and causes a session to stop responding. Addresses an issue that might cause Kerberos.dll to stop working within the Local Security Authority Subsystem Service (LSASS). This occurs when LSASS processes simultaneous Service for User (S4U) user-to-user (U2U) requests for the same client user. Addresses a known issue that might prevent recovery discs (CD or DVD) from starting if you created them using the Backup and Restore (Windows 7) app in Control Panel. This issue occurs after installing Windows updates released January 11, 2022 or later.	KB5013952	Applicable on MS4000 and Anesthesia System
Windows Malicious Software Removal Tool - v5.101	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers	KB890830	Applicable on MS4000 Console and MED3500 Console
2022-05 Security Monthly Quality Rollup for Windows Server 2008 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5012658 (released April 12, 2022) and includes new improvements for the following issues: The Key Distribution Center (KDC) code incorrectly returns error message KDC_ERR_TGT_REVOKED during Domain Controller shutdown. After installing the January 2022 Windows update or a later Windows update on the Primary Domain Controller emulator (PDCe), listing or modifying name suffixes routing by using Netdom.exe or "Active Directory Domains and Trusts" snap-in may fail and you receive the following error message: "Insufficient system resources exist to complete the requested service." The Primary Domain Controller (PDC) for the root domain incorrectly logs warning and error events in the System log when trying to scan outbound-only trusts.	KB5014010	Applicable on MS4000 Console and MED3500 Console

2022-05 Security Only Quality Update for Windows Server 2008 for x86-based Systems.	This security-only update includes new improvements for the following issues: The Key Distribution Center (KDC) code incorrectly returns error message KDC_ERR_TGT_REVOKED during Domain Controller shutdown. The Primary Domain Controller (PDC) for the root domain incorrectly logs warning and error events in the System log when trying to scan outbound-only trusts.	KB5014006	Applicable on MS4000 Console and MED3500 Console

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

bd.com

Security Patches: Security Module

May 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for May 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

Customers that maintain patches independent of BD automated delivery should ensure the validated patches are installed on their BD systems as the acting responsible entity in order to maintain the correct security posture of the system(s).

Microsoft® patches

Patch name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.101 (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	NA
2022-05 Security Only Update for .NET Framework 3.5 for Windows Server 2012 R2 for x64 (KB5013621)	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.	KB5013621	NA

2022-05 Security Only Update for .NET Framework 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows Server 2012 R2 for x64 (KB5013623)	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.	KB5013623	NA
2022-05 Security and Quality Rollup for .NET Framework 3.5 for Windows Server 2012 R2 for x64 (KB5013638)	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.	KB5013638	NA
2022-05 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 (KB5013643)	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.	KB5013643	NA
2022-05 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 (KB5013839)	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.	KB5013839	NA

2022-05 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 (KB5013872)	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.	KB5013872	NA
2022-05 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5014011)	This cumulative security update contains improvements as: • The Key Distribution Center (KDC) code incorrectly returns error message KDC_ERR_TGT_REVOKED during Domain Controller shutdown. • After installing the January 2022 Windows update or a later Windows update on the Primary Domain Controller emulator (PDCe), listing or modifying name suffixes routing by using Netdom.exe or "Active Directory Domains and Trusts" snap-in may fail and you receive the following error message: "Insufficient system resources exist to complete the requested service." • The Primary Domain Controller (PDC) for the root domain incorrectly logs warning and error events in the System log when trying to scan outbound-only trusts.	KB5014011	NA
2022-05 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 (KB5013872)	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.	KB5013872	NA

2022-05 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB5014025)	**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.**	KB5014025	**NA**
2022-05 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5013952)	This security update includes quality improvements. Key changes include: • New! Adds improvements for servicing the Secure Boot component of Windows. • Addresses an issue that might occur when you use Netdom.exe or the Active Directory Domains and Trusts snap-in to list or modify name suffixes routing. These procedures might fail. The error message is, "Insufficient system resources exist to complete the requested service." This issue occurs after installing the January 2022 security update on the primary domain controller emulator (PDCe). • Addresses an issue that causes the improper cleanup of Dynamic Data Exchange (DDE) objects. This prevents session teardown and causes a session to stop responding. • Addresses an issue that might cause Kerberos.dll to stop working within the Local Security Authority Subsystem Service (LSASS). This occurs when LSASS processes simultaneous Service for User (S4U) user-to-user (U2U) requests for the same client user. • Addresses a known issue that might prevent recovery discs (CD or DVD) from starting if you created them using the Backup and Restore (Windows 7) app in Control Panel. This issue occurs after installing Windows updates released January 11, 2022 or later.	KB5013952	NA

		KB5014026	
2022-05 Servicing Stack Update for Windows Server 2016 for x64-based Systems (KB5014026)	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.		NA

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

bd.com

Security Patches: BD Pyxis™ IV Prep

May 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for May 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

Customers that maintain patches independent of BD automated delivery should ensure the validated patches are installed on their BD systems as the acting responsible entity in order to maintain the correct security posture of the system(s).

Microsoft® patches

Patch name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.101	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	Applicable on Cato
2022-05 Servicing Stack 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.	KB5014026	Applicable on Cato

2022-05 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.	KB5013952	Applicable on Cato
2022-05 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.	KB5014011	Applicable on Cato
2022-05 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.	KB5013872	Applicable on Cato
2022-05 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.	KB5013839	Applicable on Cato
2022-05 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.	KB5014001	Applicable on Cato
2022-05 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.	KB5013872	Applicable on Cato

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

bd.com

Security Patches: BD Pharmogistics

May 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for May 2022. These patches were not found to adversely affect BD Pharmogistics products and will be applied according to customers' service agreements.

Customers that maintain patches independent of BD automated delivery should ensure the validated patches are installed on their BD systems as the acting responsible entity in order to maintain the correct security posture of the system(s).

Microsoft® patches

Patch name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	**Applicable on PLX, CII Safe and Infusion.**
2022-01 Update for Windows Server 2008 R2 for x64-based Systems (KB5010798)	This update resolves the following issues: • Active Directory attributes are not written correctly during a Lightweight Directory Access Protocol (LDAP) modify operation with multiple specific attribute changes. • Windows Servers might restart unexpectedly after installing the January 11, 2022 Windows update on domain controllers (DCs).	KB5010798	**Applicable on PLX, CII Safe and Infusion.**

2022-05 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 (KB5013872)	Security Improvements This security update addresses an issue where a local user opening a specially crafted file could cause a denial of service condition on an affected system. For more information please see CVE-2022-30130. Quality Improvements For a list of improvements that were released with this update, please see the article links in the Additional Information section of this article.	KB5013872	**Applicable on PLX, CII Safe and Infusion.**
2022-05 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB5014025)	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.	KB5014025	**Applicable on PLX, CII Safe and Infusion.**
2022-05 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 (KB5013839)	**This security update addresses an issue where a local user opening a specially crafted file could cause a denial of service condition on an affected system. For more information please see CVE-2022-30130.**	KB5013839	**Applicable on PLX, CII Safe and Infusion.**

2022-05 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5014011)	This cumulative security update contains improvements that are part of update KB5012670 (released April 12, 2022) and includes new improvements for the following issues: • The Key Distribution Center (KDC) code incorrectly returns error message KDC_ERR_TGT_REVOKED during Domain Controller shutdown.	KB5014011	**Applicable on PLX, CII Safe and Infusion.**
2022-05 Cumulative Update for Windows 10 Version 21H1 for x86-based Systems (KB5013942)	**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.**	KB5013942	**Applicable on PLX, CII Safe and Infusion.**
2022-05 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 21H1 for x64 (KB5013624)	**Security Improvements** **This security update addresses an issue where a local user opening a specially crafted file could cause a denial of service condition on an affected system. For more information please see CVE-2022-30130.** **Quality and reliability improvements** **DS1 - Addresses an issue where 3rd party .NET apps using certain System.DirectoryServices APIs crash with an Access Violation (0xC0000005).**	KB5013624	**Applicable on PLX, CII Safe and Infusion.**

Security Update for SQL Server 2016 Service Pack 1 GDR (KB4505219)	A remote code execution vulnerability exists in Microsoft SQL Server when it incorrectly handles processing of internal functions. An attacker who successfully exploited this vulnerability could execute code in the context of the SQL Server Database Engine service account. To learn more about the vulnerability, go to CVE-2019-1068.	KB4505219	**Applicable on PLX, CII Safe and Infusion.**
2022-05 Servicing Stack Update for Windows Server 2016 for x64-based Systems (KB5014026)	**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.**	KB5014026	**Applicable on PLX, CII Safe and Infusion.**

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

bd.com

Security Patches: BD Pyxis Connect

May 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for May 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

Customers that maintain patches independent of BD automated delivery should ensure the validated patches are installed on their BD systems as the acting responsible entity in order to maintain the correct security posture of the system(s).

Microsoft® patches

Patch name	Description	Patch ID	Notes
2022-05 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB5014025)	**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.** **This update applies to the following:** • **Windows 8.1 for x86-based devices** • **Windows 8.1 for x64-based devices** • **Windows RT 8.1** • **Windows Server 2012 R2** • **Windows Server 2012 R2 (Server Core installation)**	**KB5014025**	
2022-05 Security and Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows 8.1 for x64 (KB5013872)	**This security update addresses an issue where a local user opening a specially crafted file could cause a denial-of-service condition on an affected system.** **The following additional information about this update as it relates to individual product versions.** • **5013638 Description of the Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 (KB5013638)** • **5013643 Description of the Security and Quality Rollup for .NET Framework 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 (KB5013643)**	**KB5013872**	

	• **5013631 Description of the Security and Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 (KB5013631)**	
2022-05 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5014001)	**This security-only update includes new improvements for the following issues:** • **The Key Distribution Center (KDC) code incorrectly returns error message KDC_ERR_TGT_REVOKED during Domain Controller shutdown.** **The Primary Domain Controller (PDC) for the root domain incorrectly logs warning and error events in the System log when trying to scan outbound-only trusts.**	**KB5014001**
2022-05 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 (KB5013839)	**This security update addresses an issue where a local user opening a specially crafted file could cause a denial-of-service condition on an affected system.**	**KB5013839**

Windows Malicious Software Removal Tool x64 - v5.101 (KB890830)	**After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com.** ▪ **This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.**	**KB890830**
2022-05 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5014011)	**This cumulative security update contains improvements that are part of update KB5012670 (released April 12, 2022) and includes new improvements for the following issues:** • **The Key Distribution Center (KDC) code incorrectly returns error message KDC_ERR_TGT_REVOKED during Domain Controller shutdown.** • **After installing the January 2022 Windows update or a later Windows update on the Primary Domain Controller emulator (PDCe), listing or modifying name suffixes routing by using Netdom.exe or "Active Directory Domains and Trusts" snap-in may fail and you receive the following error message: "Insufficient system resources exist to complete the requested service.** • **The Primary Domain Controller (PDC) for the root domain incorrectly logs warning and error events in the System log when trying to scan outbound-only trusts.**	**KB5014011**
2022-05 Servicing Stack Update for Windows Server 2016 for x64-based Systems (KB5014026)	**This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.** **Additionally, this update adds improvements for servicing the Secure Boot component of Windows.**	**KB5014026**

2022-05 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5013952)	**This security update includes quality improvements. Key changes include:** • **New! Adds improvements for servicing the Secure Boot component of Windows.** • **Addresses an issue that might occur when you use Netdom.exe or the Active Directory Domains and Trusts snap-in to list or modify name suffixes routing. These procedures might fail. The error message is, "Insufficient system resources exist to complete the requested service." This issue occurs after installing the January 2022 security update on the primary domain controller emulator (PDCe).** • **Addresses an issue that causes the improper cleanup of Dynamic Data Exchange (DDE) objects. This prevents session teardown and causes a session to stop responding.** • **Addresses an issue that might cause Kerberos.dll to stop working within the Local Security Authority Subsystem Service (LSASS). This occurs when LSASS processes simultaneous Service for User (S4U) user-to-user (U2U) requests for the same client user.** • **Addresses a known issue that might prevent recovery discs (CD or DVD) from starting if you created them using the Backup and Restore (Windows 7) app in Control Panel. This issue occurs after installing Windows updates released January 11, 2022 or later.** **If you installed earlier updates, only the new updates contained in this package will be downloaded and installed on your device.**	**KB5013952**
2022-05 Cumulative Update for Windows 10 Version 21H2 for x64-based Systems (KB5013942)	**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.**	**KB5013942**
2022-05 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 21H1 (KB5013624)	**This security update addresses an issue where a local user opening a specially crafted file could cause a denial-of-service condition on an affected system.**	**KB5013624**

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

bd.com

Security Patches: BD Pyxis Parx

May 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for May 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

Customers that maintain patches independent of BD automated delivery should ensure the validated patches are installed on their BD systems as the acting responsible entity in order to maintain the correct security posture of the system(s).

Microsoft® patches

Patch name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.101 (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	N/A
2022-04 Cumulative Update for Windows 10 Version 1607 for x64-based Systems (KB5012596)	Updates an issue that prevents you from changing a password that has expired when you sign in to a Windows device. Updates security for your Windows operating system.	KB5012596	N/A

2022-05 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	This security update includes quality improvements. Key changes include: Adds improvements for servicing the Secure Boot component of Windows. Addresses an issue that might occur when you use Netdom.exe or the Active Directory Domains and Trusts snap-in to list or modify name suffixes routing. These procedures might fail. The error message is, "Insufficient system resources exist to complete the requested service." This issue occurs after installing the January 2022 security update on the primary domain controller emulator (PDCe). Addresses an issue that causes the improper cleanup of Dynamic Data Exchange (DDE) objects. This prevents session teardown and causes a session to stop responding. Addresses an issue that might cause Kerberos.dll to stop working within the Local Security Authority Subsystem Service (LSASS). This occurs when LSASS processes simultaneous Service for User (S4U) user-to-user (U2U) requests for the same client user. Addresses a known issue that might prevent recovery discs (CD or DVD) from starting if you created them using the Backup and Restore (Windows 7) app in Control Panel. This issue occurs after installing Windows updates released January 11, 2022 or later.	KB5013952

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

bd.com

Security Patches: BD Pyxis™ Anesthesia ES

May 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for May 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

Customers that maintain patches independent of BD automated delivery should ensure the validated patches are installed on their BD systems as the acting responsible entity in order to maintain the correct security posture of the system(s).

Microsoft® patches

Patch name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.99	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	Applicable on PAS device.

.

2022-05 Security Only Quality Update for Windows 7 for x86-based Systems.	This security-only update includes new improvements for the following issues:The Key Distribution Center (KDC) code incorrectly returns error message KDC_ERR_TGT_REVOKED during Domain Controller shutdown.The Primary Domain Controller (PDC) for the root domain incorrectly logs warning and error events in the System log when trying to scan outbound-only trusts.	KB5013999	Applicable on PAS device.
2022-05 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 an issue where a local user opening a specially crafted file could cause a denial of service condition on an affected system.	KB5013837	Applicable on PAS device.
2022-04 Security Only Update for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 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.	KB5012324	Applicable on PAS device.

2022-05 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.	KB5014102	Applicable on PAS device
Windows Malicious Software Removal Tool x64 - v5.101	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	Applicable on PAS device
2022-05 Servicing Stack Update for Windows 10 Version 1607 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.	KB5014026	Applicable on PAS device
2022-05 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.	KB5013868	Applicable on PAS device

2022-05 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.	KB5013870	Applicable on PAS device.

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

bd.com

Security Patches: BD Pyxis™ CIISafe ES

May 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for May 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

Customers that maintain patches independent of BD automated delivery should ensure the validated patches are installed on their BD systems as the acting responsible entity in order to maintain the correct security posture of the system(s).

Microsoft® patches

Patch name	Description	Patch ID	Notes
2022-05 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.	KB5013941	Applicable on CIIsafe device.
2022-05 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.	KB5013868	Applicable on CIIsafe device.

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

bd.com

Security Patches:
BD **Pyxis™ Med Station ES**

May 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for May 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

Customers that maintain patches independent of BD automated delivery should ensure the validated patches are installed on their BD systems as the acting responsible entity in order to maintain the correct security posture of the system(s).

Microsoft® patches

Patch name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.99	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	Applicable on MedSTN device.

2022-05 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.	KB5013870	Applicable on MedSTN device
2022-05 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.	KB5014102	Applicable on MedSTN device
2022-05 Security Only Quality Update for Windows 7 for x86-based Systems.	This security-only update includes new improvements for the following issues:The Key Distribution Center (KDC) code incorrectly returns error message KDC_ERR_TGT_REVOKED during Domain Controller shutdown.The Primary Domain Controller (PDC) for the root domain incorrectly logs warning and error events in the System log when trying to scan outbound-only trusts.	KB5013999	Applicable on MedSTN device
2022-05 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 an issue where a local user opening a specially crafted file could cause a denial of service condition on an affected system.	KB5013837	Applicable on MedSTN device
Security Only Update for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 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.	KB5012324	Applicable on MedSTN device

2022-05 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems.	This cumulative security update contains improvements that are part of update KB5012626 (released April 12, 2022) and includes new improvements for the following issues: The Key Distribution Center (KDC) code incorrectly returns error message KDC_ERR_TGT_REVOKED during Domain Controller shutdown. After installing the January 2022 Windows update or a later Windows update on the Primary Domain Controller emulator (PDCe), listing or modifying name suffixes routing by using Netdom.exe or "Active Directory Domains and Trusts" snap-in may fail and you receive the following error message: "Insufficient system resources exist to complete the requested service." The Primary Domain Controller (PDC) for the root domain incorrectly logs warning and error events in the System log when trying to scan outbound-only trusts.	KB5014012	Applicable on MedSTN device
2022-05 Servicing Stack Update for Windows 10 Version 1607 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.	KB5014026	Applicable on MedSTN device
2022-05 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.	KB5013625	Applicable on MedSTN device
Windows Malicious Software Removal Tool x64 - v5.101	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. This update makes quality improvements to the servicing stack, which is the component that installs	KB890830	Applicable on MedSTN device

2022-05 Servicing Stack Update for Windows Server 2016 for x64-based Systems.	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.	KB5014026	Applicable on MedSTN device
2022-05 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.	KB5013868	Applicable on MedSTN device

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

Security Patches: BD Pyxis™ Supply

May 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for May 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

Customers that maintain patches independent of BD automated delivery should ensure the validated patches are installed on their BD systems as the acting responsible entity in order to maintain the correct security posture of the system(s).

Microsoft® patches

Patch name	Description	Patch ID	Notes
2022-05 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems	This cumulative security update contains improvements that are part of update KB5012670 (released April 12, 2022) and includes new improvements for the following issues: • The Key Distribution Center (KDC) code incorrectly returns error message KDC_ERR_TGT_REVOKED during Domain Controller shutdown. • After installing the January 2022 Windows update or a later Windows update on the Primary Domain Controller emulator (PDCe), listing or modifying name suffixes routing by using Netdom.exe or "Active Directory Domains and Trusts" snap-in may fail and you receive the following error message: "Insufficient system resources exist to complete the requested service." • The Primary Domain Controller (PDC) for the root domain incorrectly logs warning and error events in the System log when trying to scan outbound-only trusts.	KB5014011	Applicable on Supply.

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

bd.com

2022-05 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 (KB5013839)	This security update addresses an issue where a local user opening a specially crafted file could cause a denial of service condition on an affected system. For more information please see CVE-2022-30130.	KB5013839	Applicable on Supply.
2022-05 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5014001)	This security-only update includes new improvements for the following issues: • The Key Distribution Center (KDC) code incorrectly returns error message KDC_ERR_TGT_REVOKED during Domain Controller shutdown. • The Primary Domain Controller (PDC) for the root domain incorrectly logs warning and error events in the System log when trying to scan outbound-only trusts.	KB5014001	Applicable on Supply.
2022-05 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 (KB5013872)	This security update addresses an issue where a local user opening a specially crafted file could cause a denial of service condition on an affected system. For more information please see CVE-2022-30130.	KB5013872	Applicable on Supply.
2022-05 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB5014025)	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.	KB5014025	Applicable on Supply.

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

bd.com

2022-05 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x64-based Systems (KB5014012)	This cumulative security update contains improvements that are part of update KB5012626 (released April 12, 2022) and includes new improvements for the following issues: • The Key Distribution Center (KDC) code incorrectly returns error message KDC_ERR_TGT_REVOKED during Domain Controller shutdown. • After installing the January 2022 Windows update or a later Windows update on the Primary Domain Controller emulator (PDCe), listing or modifying name suffixes routing by using Netdom.exe or "Active Directory Domains and Trusts" snap-in may fail and you receive the following error message: "Insufficient system resources exist to complete the requested service." • The Primary Domain Controller (PDC) for the root domain incorrectly logs warning and error events in the System log when trying to scan outbound-only trusts.	KB5014012	Applicable on Supply.
2022-05 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 for x86 (KB5013870)	This security update addresses an issue where a local user opening a specially crafted file could cause a denial of service condition on an affected system. For more information please see CVE-2022-30130.	KB5013870	Applicable on Supply.
2022-05 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 for x86 (KB5013837)	This security update addresses an issue where a local user opening a specially crafted file could cause a denial of service condition on an affected system. For more information please see CVE-2022-30130.	KB5013837	Applicable on Supply.

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

bd.com

2022-05 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems (KB5013999)	This security-only update includes new improvements for the following issues: • The Key Distribution Center (KDC) code incorrectly returns error message KDC_ERR_TGT_REVOKED during Domain Controller shutdown. • The Primary Domain Controller (PDC) for the root domain incorrectly logs warning and error events in the System log when trying to scan outbound-only trusts.	KB5013999	Applicable on Supply.
2022-05 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5013952)	This security update includes quality improvements. Key changes include: • New! Adds improvements for servicing the Secure Boot component of Windows. • Addresses an issue that might occur when you use Netdom.exe or the Active Directory Domains and Trusts snap-in to list or modify name suffixes routing. These procedures might fail. The error message is, "Insufficient system resources exist to complete the requested service." This issue occurs after installing the January 2022 security update on the primary domain controller emulator (PDCe). • Addresses an issue that causes the improper cleanup of Dynamic Data Exchange (DDE) objects. This prevents session teardown and causes a session to stop responding. • Addresses an issue that might cause Kerberos.dll to stop working within the Local Security Authority Subsystem Service (LSASS). This occurs when LSASS processes simultaneous Service for User (S4U) user-to-user (U2U) requests for the same client user. • Addresses a known issue that might prevent recovery discs (CD or DVD) from starting if you created them using the Backup and Restore (Windows 7) app in Control Panel. This issue occurs after installing Windows updates released January 11, 2022 or later.	KB5013952	Applicable on Supply.

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

bd.com

2022-05 Servicing Stack Update for Windows Server 2016 for x64-based Systems (KB5014026)	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates. Additionally, this update adds improvements for servicing the Secure Boot component of Windows.	KB5014026	Applicable on Supply.
2022-05 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB5013941)	This security update includes improvements that were a part of update KB5012636 (released April 21, 2022) and also addresses the following issues: • This update contains miscellaneous security improvements to internal OS functionality. No additional issues were documented for this release.	KB5013941	Applicable on Supply.
2022-05 Cumulative Update for Windows Server 2019 for x64-based Systems (KB5013941)	This security update includes improvements that were a part of update KB5012636 (released April 21, 2022) and also addresses the following issues: This update contains miscellaneous security improvements to internal OS functionality. No additional issues were documented for this release.	KB5013941	Applicable on Supply.
2022-05 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10 Version 1809 for x64 (KB5013868)	This security update addresses an issue where a local user opening a specially crafted file could cause a denial of service condition on an affected system. For more information please see CVE-2022-30130.	KB5013868	Applicable on Supply.
2022-05 Cumulative Update for .NET Framework 3.5 and 4.7.2 for Windows Server 2019 for ARM64 (KB5013868)	This security update addresses an issue where a local user opening a specially crafted file could cause a denial of service condition on an affected system. For more information please see CVE-2022-30130.	KB5013868	Applicable on Supply.
Windows Malicious Software Removal Tool x64 - v5.101	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