Security Patches:
BD Pyxis™ Anesthesia System 3500

January 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for January 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
2023-01 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5021291 (released December 13, 2022). This update also makes improvements for the following issues: • Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. • Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server	KB5022338	Applicable on 3500 Anesthesia System and MS3500 Station
2023-01 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This update makes improvements for the following issues: ▪ Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. ▪ Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.	KB5022339	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

January 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for January 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	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS 4000 Console and MS4000 Anesthesia and Station
2023-01 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	This security update includes quality improvements. When you install this KB: ▪ New! This update provides the Quick Assist application for your client device. ▪ This update addresses an issue that might affect authentication. It might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if you do not set the encryption types or you disable the RC4 encryption type on the domain. ▪ This update addresses an issue that affects cluster name objects (CNO) or virtual computer objects (VCO). Password reset fails. The error message is, "There was an error resetting the ADpassword... // 0x80070005". ▪ This update introduces a Group Policy that enables and disables HTML Application (HTA) files. If you enable this policy, it stops you from running HTA files. If you disable or do not configure this policy, you can run HTA file.	KB5022289	Applicable on 3500/MS4000 Anesthesia System and MS3500 /MS4000 Station

2023-01 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5021291 (released December 13, 2022). This update also makes improvements for the following issues: ▪ Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. ▪ Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.	KB5022338	Applicable on 3500 Anesthesia System and MS3500 Station
2023-01 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This update makes improvements for the following issues: ▪ Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. ▪ Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.	KB5022339	Applicable on 3500 Anesthesia System and MS3500 Station

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

bd.com

Security Patches: BD Pyxis CIISafe

January 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for January 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
2023-01 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.	KB5022289	Applicable to CIISafe device.
2023-01 Security Monthly Quality Rollup for Windows Server 2008 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.	KB5022338	Applicable to CIISafe device.

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

bd.com

Security Patches:
BD Pyxis™ MedStation™ 3500

January 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for January 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 - v5.109	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS3500 and MS4000 Console
2023-01 Security Only Quality Update for Windows Server 2008 for x86-based Systems	This update makes improvements for the following issues: ▪ Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. ▪ Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.	KB5022353	Applicable on MS3500 and MS4000 Console
2023-01 Security Monthly Quality Rollup for Windows Server 2008 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5021289 (released December 13, 2022). This update also makes improvements for the following issues: ▪ Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. ▪ Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases.	KB5022340	Applicable on MS3500 and MS4000 Console

	The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.		
2023-01 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5021291 (released December 13, 2022). This update also makes improvements for the following issues: ▪ Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. ▪ Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.	KB5022338	Applicable on 3500 Anesthesia System and MS3500 Station
2023-01 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This update makes improvements for the following issues: ▪ Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. ▪ Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.	KB5022339	Applicable on 3500 Anesthesia System and MS3500 Station

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

bd.com

Security Patches:
BD Pyxis™ MedStation™ 4000

January 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for January 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 - v5.109	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS3500 and MS 4000 Console
2023-01 Security Only Quality Update for Windows Server 2008 for x86-based Systems	This update makes improvements for the following issues: ▪ Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. ▪ Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.	KB5022353	Applicable on MS3500 and MS4000 Console
2023-01 Security Monthly Quality Rollup for Windows Server 2008 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5021289 (released December 13, 2022). This update also makes improvements for the following issues: ▪ Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. ▪ Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.	KB5022340	Applicable on MS3500 and MS4000 Console

2023-01 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5021291 (released December 13, 2022). This update also makes improvements for the following issues: ▪ Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. ▪ Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.	KB5022338	Applicable on 3500 Anesthesia System and MS3500 Station
2023-01 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This update makes improvements for the following issues: ▪ Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. ▪ Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.	KB5022339	Applicable on 3500 Anesthesia System and MS3500 Station
Windows Malicious Software Removal Tool x64 - v5.109	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS 4000 Console and MS4000 Anesthesia and Station
2023-01 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	This security update includes quality improvements. When you install this KB: ▪ New! This update provides the Quick Assist application for your client device. ▪ This update addresses an issue that might affect authentication. It might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if you do not set the encryption types or you disable the RC4 encryption type on the domain. ▪ This update addresses an issue that affects cluster name objects (CNO) or virtual computer objects (VCO). Password reset fails. The error message is, "There was an error resetting the ADpassword... // 0x80070005". ▪ This update introduces a Group Policy that enables and disables HTML Application (HTA) files. If you enable this policy, it stops you from running HTA files. If you disable or do not configure this policy, you can run HTA file.	KB5022289	Applicable on 3500/MS4000 Anesthesia System and MS3500 /MS4000 Station

2023-01 Cumulative Update for Windows Server 2016 for x64-based Systems	This update addresses security issues for your Windows operating system.	KB5022289	Applicable on MS4000 Anesthesia System, MS4000 Station and console

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

bd.com

Security Patches: Security Module

January 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for January 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.
2023-01 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5022346)	This update makes improvements for the following issues: • Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. • Starting in this release, we are displaying a modal dialog box to remind users about the End of Support for Windows 8.1 in January 2023. This reminder does not appear on managed devices that run Windows 8.1 Pro or Windows 8.1 Enterprise.	KB5022346	Applicable on Security Module devices.

2023-01 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5022352)	This cumulative security update includes improvements that are part of update KB5021294 (released December 13, 2022). This update also makes improvements for the following issues: • Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. • Starting in this release, we are displaying a modal dialog box to remind users about the End of Support for Windows 8.1 in January 2023. This reminder does not appear on managed devices that run Windows 8.1 Pro or Windows 8.1 Enterprise.	KB5022352	Applicable on Security Module devices.
2023-01 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5022289)	This security update includes quality improvements. When you install this KB: • New! This update provides the Quick Assist application for your client device. • This update addresses an issue that might affect authentication. It might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if you do not set the encryption types or you disable the RC4 encryption type on the domain.	KB5022289	Applicable on Security Module devices.

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

bd.com

Security Patches: BD Pyxis™ IV Prep

January 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for January 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
2023-01 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.	KB5022289	Applicable on Cato

2023-01 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.	KB5022352	Applicable on Cato
2023-01 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	KB5022346	Applicable on Cato

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

bd.com

Security Patches: BD Pyxis Connect

January 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for January 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
2023-01 Cumulative Update for Windows Server 2016 for x64-based Systems	This update addresses security issues for your Windows operating system.	KB5022289	N/A
2023-01 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems	This update makes improvements for the following issues: • Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. • Starting in this release, we are displaying a modal dialog box to remind users about the End of Support for Windows 8.1 in January 2023. This reminder does not appear on managed devices that run Windows 8.1 Pro or Windows 8.1 Enterprise. • Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.	KB5022346	N/A
Windows Malicious Software Removal Tool x64 - v5.107	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

2023-01 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems	This cumulative security update includes improvements for the following issues: • Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. • Starting in this release, we are displaying a modal dialog box to remind users about the End of Support for Windows 8.1 in January 2023. This reminder does not appear on managed devices that run Windows 8.1 Pro or Windows 8.1 Enterprise. • Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.	KB5022352	N/A
2023-01 Cumulative Update for Windows 10 Version 22H2 for x64-based Systems	This update addresses security issues for your Windows operating system.	KB5019275	N/A
2023-01 Cumulative Update Preview for Windows 10 Version 22H2 for x64-based Systems	This update includes the following: • It displays storage alerts for Microsoft OneDrive subscribers on the Systems page in the Settings app. The alerts appear when you are close to your storage limit. You can also manage your storage and purchase additional storage, if needed. • It addresses an issue that might affect news and interests. It might flicker on the taskbar and File Explorer might stop responding.	KB5022282	N/A
2023-01 Cumulative Update Preview for .Net Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2 for x64-based Systems	There are no new security improvements in this release. This update is cumulative and contains all previously released security improvements.	KB5022478	N/A

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

bd.com

Security Patches: BD Pharmogistics

January 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for January 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.
2023-01 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems.	This cumulative security update includes improvements that are part of update KB5021294 (released December 13, 2022). This update also makes improvements for the following issues: Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain.	KB5022352	N/A

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

bd.com

	Starting in this release, we are displaying a modal dialog box to remind users about the End of Support for Windows 8.1 in January 2023. This reminder does not appear on managed devices that run Windows 8.1 Pro or Windows 8.1 Enterprise. Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.		
2023-01 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems	This cumulative security update contains improvements that are part of update KB5021291 (released December 13, 2022). This update also makes improvements for the following issues: Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.	KB5022338	N/A
2023-01 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.	KB5022282	N/A

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

bd.com

2023-01 Cumulative Update for Windows Server 2016 for x64-based Systems	Improvements This security update includes quality improvements. When you install this KB: New! This update provides the Quick Assist application for your client device. This update addresses an issue that might affect authentication. It might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if you do not set the encryption types or you disable the RC4 encryption type on the domain. This update addresses an issue that affects cluster name objects (CNO) or virtual computer objects (VCO). Password reset fails. The error message is, "There was an error resetting the AD password... // 0x80070005”. This update introduces a Group Policy that enables and disables HTML Application (HTA) files. If you enable this policy, it stops you from running HTA files. If you disable or do not configure this policy, you can run HTA file.	KB5022289	N/A

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

bd.com

Security Patches: PARx

Jan 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for Jan 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	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
2023-01 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	2023-01 Cumulative Update for Windows 10 Version 1607 for x64-based Systems improves the security of Windows Components and Microsoft Services. Windows 10 1607 users may now use the Quick Assist application on all their client devices. Introduces a new Group Policy for enabling or disabling HTML Application (HTA) files. If you enable this policy, it stops you from running HTA files. However, when you disable or leave this policy not configured, you can run the HTA file. To know more about this, follow the below section.	KB5022289	Applicable on ParX

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

bd.com

Security Patches: TIM

Jan 2023

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

	Windows Defender Offline or Microsoft Safety Scanner. This article contains information about how the tool differs from an antivirus or antimalware product, how you can download and run the tool, what happens when the tool finds malware, and tool release information. It also includes information for the administrators and advanced users, including information about supported command-line switches. This security update addresses a vulnerability where restricted mode is triggered for the parsing of XPS files, preventing gadget chains which could allow remote code execution on an affected system. For more information please see CVE-2022-41089. Quality and Reliability Improvements There are no new Quality and Reliability Improvements in this update.		
VMware, Inc. - Net - 1.9.11.0	Windows Server 2016 and Later Servicing Drivers	1.9.11.0	Applicable on TIM.
2023-01 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5022289)	This security update includes quality improvements. When you install this KB: New! This update provides the Quick Assist application for your client device. This update addresses an issue that might affect authentication. It might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if you do not set the encryption types or you disable the RC4 encryption type on the domain.	KB5022289	Applicable on TIM.

This update addresses an issue that affects cluster name objects (CNO) or virtual computer objects (VCO). Password reset fails.

The error message is, "There was an error resetting the AD password... // 0x80070005”.

This update introduces a Group Policy that enables and disables HTML Application (HTA) files. If you enable this policy, it stops you from running HTA files.
If you disable or do not configure this policy, you can run HTA file. To configure this Group Policy:

Open the Group Policy Editor.

Select Computer Configuration > Administrative Templates > Windows Components > Internet Explorer.

Double-click Turn on DisableHTMLApplication.
Select Enabled.

To save the policy setting, select OK or Apply.

This update addresses a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases.

The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.

2023-01 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems	This cumulative security update includes improvements that are part of update KB5021294 (released December 13, 2022). This update also makes improvements for the following issues: Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. Starting in this release, we are displaying a modal dialog box to remind users about the End of Support for Windows 8.1 in January 2023. This reminder does not appear on managed devices that run Windows 8.1 Pro or Windows 8.1 Enterprise. Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server. For more information about the resolved security vulnerabilities, please refer to the Deployments | Security Update Guide and the January 2023 Security Updates.	KB5022352	Applicable on TIM.
2023-01 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems	This update makes improvements for the following issues: Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. Starting in this release, we are displaying a modal dialog box to remind users about the End of Support for Windows 8.1 in January 2023. This reminder does not appear on managed devices that run Windows 8.1 Pro or Windows 8.1 Enterprise. Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL	KB5022346	Applicable on TIM.

Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.

For more information about the resolved security vulnerabilities, please refer to the Deployments | Security Update Guide and the January 2023 Security Updates.

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

bd.com

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

January 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for January 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
2023-01 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.	KB5022338	Applicable on PAS device.
2023-01 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.	KB5022339	Applicable on PAS device.
2023-01 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	KB5022289	Applicable on PAS device.

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 PAS device.
2023-01 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.	KB5022286	Applicable on PAS device.

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

bd.com

Security Patches: BD Pyxis™ CIISafe ES

January 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for January 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
2023-01 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.	KB5022286	Applicable on CIISafe device.
2023-01 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.	KB5022282	Applicable on CIISafe device.

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 CIISafe device.**

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

bd.com

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

January 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for January 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
2023-01 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.	KB5022339	Applicable on Medstn ES device.
2023-01 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.	KB5022338	Applicable on Medstn ES device.

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 Medstn ES device.
2023-01 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.	KB5022289	Applicable on Medstn ES device.
2023-01 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.	KB5022286	Applicable on Medstn ES device.

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

bd.com

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

January 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for January 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
2023-01 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.	KB5022286	Applicable on 1.7.1,1.7.2,1.7.3, PAS device.
2023-01 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.	KB5022282	Applicable on 1.7.1,1.7.2,1.7.3, PAS device.

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 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™ ES Server**

January 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for January 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
2023-01 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.	KB5022286	Applicable on 1.7.1,1.7.2.,1.7.3, ES Server.
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 1.7.1,1.7.2.,1.7.3, ES Server.

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

bd.com

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

January 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for January 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
2023-01 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.	KB5022286	Applicable on 1.7.1,1.7.2,1.7.3, Med Stn device.
2023-01 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.	KB5022282	Applicable on 1.7.1,1.7.2,1.7.3, Med Stn device.

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 1.7.1,1.7.2,1.7.3, Med Stn device.

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

bd.com

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

January 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for January 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
2023-01 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.	KB5022352	Applicable on MedES Server.
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 MedES Server.

2023-01 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.	KB5022346	Applicable on MedES Server.
2023-01 Security Only Quality Update for Windows Server 2008 for x86-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5022353	Applicable on MedES Server.
2023-01 Security Monthly Quality Rollup for Windows Server 2008 for x64-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5022340	Applicable on MedES Server.
2023-01 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.	KB5022289	Applicable on MedES Server.

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

bd.com

Security Patches: BD Pyxis™ Supply

January 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for January 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
2023-01 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems (KB5022338)	This cumulative security update contains improvements that are part of update KB5021291 (released December 13, 2022). This update also makes improvements for the following issues: • Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. • Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.	KB5022338	Applicable on Supply.
2023-01 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems (KB5022339))	This update makes improvements for the following issues: • Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. • Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an	KB5022339	Applicable on Supply.

	error in the app, or you might receive an error from the SQL Server.		
2023-01 Security Only Quality Update for Windows Server 2008 for x86-based Systems (KB5022353)	This update makes improvements for the following issues: • Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. • Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.	KB5022353	Applicable on Supply.
2023-01 Security Monthly Quality Rollup for Windows Server 2008 for x86-based Systems (KB5022340)	This cumulative security update contains improvements that are part of update KB5021289 (released December 13, 2022). This update also makes improvements for the following issues: • Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. • Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.	KB5022340	Applicable on Supply.
2023-01 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5022346)	This update makes improvements for the following issues: • Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. • Starting in this release, we are displaying a modal dialog box to remind users about the End of Support for Windows 8.1 in January 2023. This reminder does not appear on managed devices that run Windows 8.1 Pro or Windows 8.1 Enterprise. • Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.	KB5022346	Applicable on Supply.

2023-01 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5022352)	This cumulative security update includes improvements that are part of update KB5021294 (released December 13, 2022). This update also makes improvements for the following issues: • Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. • Starting in this release, we are displaying a modal dialog box to remind users about the End of Support for Windows 8.1 in January 2023. This reminder does not appear on managed devices that run Windows 8.1 Pro or Windows 8.1 Enterprise. • Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.	KB5022352	Applicable on Supply.
2023-01 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems (KB5022339)	This update makes improvements for the following issues: • Authentication might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if encryption types are not set or if RC4 Encryption type is disabled on the domain. • Resolves a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.	KB5022339	Applicable on Supply.
2021-12 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5008207)	This security update includes quality improvements. Key changes include: • Adds support for the cancellation of daylight savings time for the Republic of Fiji for 2021. • Addresses a known issue that causes error codes 0x000006e4, 0x0000007c, or 0x00000709 when connecting to a remote printer that is shared on a Windows print server. • Addresses a known issue that might prevent apps, such as Kaspersky apps, from opening after you attempt to repair or update the apps using the Microsoft Installer (MSI).	KB5008207	Applicable on Supply.

2022-12 Cumulative Update for .NET Framework 4.8 for Windows Server 2016 for x64 (KB5020873)	This security update addresses a vulnerability where restricted mode is triggered for the parsing of XPS files, preventing gadget chains which could allow remote code execution on an affected system. For more information please see CVE-2022-41089.	KB5020873	Applicable on Supply.
2022-12 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5021235)	This security update includes quality improvements. When you install this KB: • This update addresses a known issue that might affect the Local Security Authority Subsystem Service (LSASS.exe). It might leak memory on Windows domain controllers. This issue might occur when you install Windows updates dated November 8, 2022, or later.	KB5021235	Applicable on Supply.
2022-08 Security Update for Windows Server 2016 for x64-based Systems (KB5012170)	This security update makes improvements to Secure Boot DBX for the supported Windows versions listed in the "Applies to" section. Key changes include the following: • Windows devices that has Unified Extensible Firmware Interface (UEFI) based firmware can run with Secure Boot enabled. The Secure Boot Forbidden Signature Database (DBX) prevents UEFI modules from loading. This update adds modules to the DBX. A security feature bypass vulnerability exists in secure boot. An attacker who successfully exploited the vulnerability might bypass secure boot and load untrusted software. This security update addresses the vulnerability by adding the signatures of the known vulnerable UEFI modules to the DBX.	KB5012170	Applicable on Supply.

2023-01 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5022289)	This security update includes quality improvements. When you install this KB:
	• New! This update provides the Quick Assist application for your client device.
	• This update addresses an issue that might affect authentication. It might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if you do not set the encryption types or you disable the RC4 encryption type on the domain.
	• This update addresses an issue that affects cluster name objects (CNO) or virtual computer objects (VCO). Password reset fails. The error message is, "There was an error resetting the AD password... // 0x80070005".
	• This update introduces a Group Policy that enables and disables HTML Application (HTA) files. If you enable this policy, it stops you from running HTA files. If you disable or do not configure this policy, you can run HTA file. To configure this Group Policy:
	  ○ Open the Group Policy Editor.
	  ○ Select Computer Configuration > Administrative Templates > Windows Components > Internet Explorer.
	  ○ Double-click Turn on DisableHTMLApplication.
	  ○ Select Enabled.
	  ○ To save the policy setting, select OK or Apply.
	• This update addresses a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.
		KB5022289	Applicable on Supply.

2023-01 Cumulative Update for Windows Server 2019 for x64-based Systems (KB5022286)	This security update includes improvements. When you install this KB: • New! This update provides the Quick Assist application for your client device. • This update addresses an issue that might affect authentication. It might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if you do not set the encryption types or you disable the RC4 encryption type on the domain. • This update addresses an issue that affects cluster name objects (CNO) or virtual computer objects (VCO). Password reset fails. The error message is, "There was an error resetting the AD password... // 0x80070005".	KB5022286	Applicable on Supply.

	• This update addresses an issue that affects Microsoft Defender for Endpoint. Automated investigation blocks live response investigations. • This update addresses a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.		
2023-01 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB5022286)	This security update includes improvements. When you install this KB: • New! This update provides the Quick Assist application for your client device. • This update addresses an issue that might affect authentication. It might fail after you set the higher 16-bits of the msds-SupportedEncryptionTypes attribute. This issue might occur if you do not set the encryption types or you disable the RC4 encryption type on the domain. • This update addresses an issue that affects cluster name objects (CNO) or virtual computer objects (VCO). Password reset fails. The error message is, "There was an error resetting the AD password... // 0x80070005". • This update addresses an issue that affects Microsoft Defender for Endpoint. Automated investigation blocks live response investigations. • This update addresses a known issue that affects apps that use Microsoft Open Database Connectivity (ODBC) SQL Server Driver (sqlsrv32.dll) to connect to databases. The connection might fail. You might also receive an error in the app, or you might receive an error from the SQL Server.	KB5022286	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.

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

bd.com