Security Patches: BD Pyxis™ Anesthesia System 3500

November 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for November 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
2022-11 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5019958	Applicable on 3500 Anesthesia System and MS3500 Station
2022-11 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5017361 (released October 11, 2022) and includes key changes for the following: Addresses a Distributed Component Object Model (DCOM) authentication hardening issue to automatically raise authentication level for all non-anonymous activation requests from DCOM clients. This will occur if the authentication level is less than RPC_C_AUTHN_LEVEL_PKT_INTEGRITY. Updates the daylight-saving time (DST) for Jordan to prevent moving the clock back 1 hour on October 28, 2022. Additionally, changes the display name of Jordan standard time from "(UTC+02:00) Amman" to "(UTC+03:00) Amman". Addresses an issue where Microsoft Azure Active Directory (AAD) Application Proxy Connector cannot retrieve a Kerberos ticket on behalf of the user because of the following general API error: "The handle specified is invalid (0x80090301)."	KB5020000	Applicable on 3500 Anesthesia System and MS3500 Station

2022-11 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This security-only update includes key changes for the following: ▪ Updates the daylight-saving time (DST) for Jordan to prevent moving the clock back 1 hour on October 28, 2022. Additionally, changes the display name of Jordan standard time from "(UTC+02:00) Amman" to "(UTC+03:00) Amman". ▪ Addresses an issue where, after installing the January 11, 2022 or later update, the Forest Trust creation process fails to populate the DNS name suffixes into the trust information attributes.	KB5020013	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

November 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for November 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 - v5.107	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS4000 Console, Anesthesia System and Station
2022-11 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	It stops the start of daylight saving time in Jordan at the end of October 2022. The Jordan time zone will permanently shift to the UTC + 3 time zone. It addresses security issues for your Windows operating system.	KB5019964	Applicable on MS4000 Console
2022-11 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5019958	Applicable on 3500 Anesthesia System and MS3500 Station
2022-11 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This security-only update includes key changes for the following: Updates the daylight-saving time (DST) for Jordan to prevent moving the clock back 1 hour on October 28, 2022. Additionally, changes the display name of Jordan standard time from "(UTC+02:00) Amman" to "(UTC+03:00) Amman". Addresses an issue where, after installing the January 11, 2022 or later update, the Forest Trust creation process fails to populate the DNS name suffixes into the trust information attributes.	KB5020013	Applicable on 3500 Anesthesia System and MS3500 Station

2022-11 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5017361 (released October 11, 2022) and includes key changes for the following: Addresses a Distributed Component Object Model (DCOM) authentication hardening issue to automatically raise authentication level for all non-anonymous activation requests from DCOM clients. This will occur if the authentication level is less than RPC_C_AUTHN_LEVEL_PKT_INTEGRITY. Updates the daylight-saving time (DST) for Jordan to prevent moving the clock back 1 hour on October 28, 2022. Additionally, changes the display name of Jordan standard time from "(UTC+02:00) Amman" to "(UTC+03:00) Amman". Addresses an issue where Microsoft Azure Active Directory (AAD) Application Proxy Connector cannot retrieve a Kerberos ticket on behalf of the user because of the following general API error: "The handle specified is invalid (0x80090301)."	KB5020000	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

November 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for November 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
2022-11 Security Monthly Quality Rollup for Windows Embedded Standard 7 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.	KB 5020000	Applicable to CIISafe device.
2022-11 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.	KB5020688	Applicable to CIISafe device.
2022-11 Cumulative Security Update for Internet Explorer 11 for Windows 7 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	KB5019958	Applicable to CIISafe device

2022-11 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.	KB5019964	Applicable to CIISafe device.
2022-11 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.	KB5020614	Applicable to CIISafe device

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

bd.com

Security Patches: BD Pyxis™ MedStation™ 3500

November 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for November 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 - v5.107	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS3500 and MS 4000 Console
2022-11 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.	KB5020005	Applicable on MS3500 and MS 4000 Console
2022-11 Security Only Quality Update for Windows Server 2008 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5017361 (released October 11, 2022) and includes key changes for the following: Addresses a Distributed Component Object Model (DCOM) authentication hardening issue to automatically raise authentication level for all non-anonymous activation requests from DCOM clients. This will occur if the authentication level is less than RPC_C_AUTHN_LEVEL_PKT_INTEGRITY. Updates the daylight-saving time (DST) for Jordan to prevent moving the clock back 1 hour on October 28, 2022. Additionally, changes the display name of Jordan standard time from "(UTC+02:00) Amman" to "(UTC+03:00) Amman".	KB5020019	Applicable on MS3500 and MS 4000 Console
2022-11 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5019958	Applicable on 3500 Anesthesia System and MS3500 Station

2022-11 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5017361 (released October 11, 2022) and includes key changes for the following: Addresses a Distributed Component Object Model (DCOM) authentication hardening issue to automatically raise authentication level for all non-anonymous activation requests from DCOM clients. This will occur if the authentication level is less than RPC_C_AUTHN_LEVEL_PKT_INTEGRITY. Updates the daylight-saving time (DST) for Jordan to prevent moving the clock back 1 hour on October 28, 2022. Additionally, changes the display name of Jordan standard time from "(UTC+02:00) Amman" to "(UTC+03:00) Amman". Addresses an issue where Microsoft Azure Active Directory (AAD) Application Proxy Connector cannot retrieve a Kerberos ticket on behalf of the user because of the following general API error: "The handle specified is invalid (0x80090301)."	KB5020000	Applicable on 3500 Anesthesia System and MS3500 Station
2022-11 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This security-only update includes key changes for the following: ▪ Updates the daylight-saving time (DST) for Jordan to prevent moving the clock back 1 hour on October 28, 2022. Additionally, changes the display name of Jordan standard time from "(UTC+02:00) Amman" to "(UTC+03:00) Amman". ▪ Addresses an issue where, after installing the January 11, 2022 or later update, the Forest Trust creation process fails to populate the DNS name suffixes into the trust information attributes.	KB5020013	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

November 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for November 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 - v5.107	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS4000 Console, Anesthesia System and Station
2022-11 Cumulative Update for Windows Server 2016 for x64-based Systems	It stops the start of daylight saving time in Jordan at the end of October 2022. The Jordan time zone will permanently shift to the UTC + 3 time zone. It addresses security issues for your Windows operating system.	KB5019964	Applicable on MS4000 Console
Windows Malicious Software Removal Tool - v5.107	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS3500 and MS 4000 Console
2022-11 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	It stops the start of daylight saving time in Jordan at the end of October 2022. The Jordan time zone will permanently shift to the UTC + 3 time zone. It addresses security issues for your Windows operating system.	KB5019964	Applicable on MS4000 Console

2022-11 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5019958	Applicable on 3500 Anesthesia System and MS3500 Station
2022-11 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This security-only update includes key changes for the following: ▪ Updates the daylight-saving time (DST) for Jordan to prevent moving the clock back 1 hour on October 28, 2022. Additionally, changes the display name of Jordan standard time from "(UTC+02:00) Amman" to "(UTC+03:00) Amman". ▪ Addresses an issue where, after installing the January 11, 2022 or later update, the Forest Trust creation process fails to populate the DNS name suffixes into the trust information attributes.	KB5020013	Applicable on 3500 Anesthesia System and MS3500 Station
2022-11 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5017361 (released October 11, 2022) and includes key changes for the following: Addresses a Distributed Component Object Model (DCOM) authentication hardening issue to automatically raise authentication level for all non-anonymous activation requests from DCOM clients. This will occur if the authentication level is less than RPC_C_AUTHN_LEVEL_PKT_INTEGRITY. Updates the daylight-saving time (DST) for Jordan to prevent moving the clock back 1 hour on October 28, 2022. Additionally, changes the display name of Jordan standard time from "(UTC+02:00) Amman" to "(UTC+03:00) Amman". Addresses an issue where Microsoft Azure Active Directory (AAD) Application Proxy Connector cannot retrieve a Kerberos ticket on behalf of the user because of the following general API error: "The handle specified is invalid (0x80090301)."	KB5020000	Applicable on 3500 Anesthesia System and MS3500 Station
2022-11 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.	KB5020005	Applicable on MS3500 and MS 4000 Console

2022-11 Security Only Quality Update for Windows Server 2008 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5017361 (released October 11, 2022) and includes key changes for the following: Addresses a Distributed Component Object Model (DCOM) authentication hardening issue to automatically raise authentication level for all non-anonymous activation requests from DCOM clients. This will occur if the authentication level is less than RPC_C_AUTHN_LEVEL_PKT_INTEGRITY. Updates the daylight-saving time (DST) for Jordan to prevent moving the clock back 1 hour on October 28, 2022. Additionally, changes the display name of Jordan standard time from “(UTC+02:00) Amman” to “(UTC+03:00) Amman”.	KB5020019	Applicable on MS3500 and MS 4000 Console

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

bd.com

Security Patches: Security Module

November 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for November 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 - v5.105 (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.
2022-11 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems (KB5019958)	If you use update management processes other than Windows Update and you automatically approve all security update classifications for deployment, this update, the November 2022 Security Only Quality Update, and the November 2022 Security Monthly Quality Rollup are deployed. We recommend that you review your update deployment rules to make sure that the desired updates are deployed	KB5019958	Applicable on Security Module devices.
2022-11 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5020023)	This cumulative security update includes improvements that are part of update KB5018474 (released October 11, 2022) and includes key changes for the following: • Addresses a Distributed Component Object Model (DCOM) authentication hardening issue to automatically raise authentication level for all non-anonymous activation requests from DCOM clients. This will occur if the authentication level is less than RPC_C_AUTHN_LEVEL_PKT_INTEGRITY.	KB5020023	Applicable on Security Module devices.

2022-11 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5020010)	This security-only update includes key changes for the following: • Updates the daylight-saving time (DST) for Jordan to prevent moving the clock back 1 hour on October 28, 2022. Additionally, changes the display name of Jordan standard time from "(UTC+02:00) Amman" to "(UTC+03:00) Amman". • Addresses an issue where, after installing the January 11, 2022 or later update, the Forest Trust creation process fails to populate the DNS name suffixes into the trust information attributes.	KB5020010	Applicable on Security Module devices.
2022-11 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 (KB5020690)	This security update addresses a vulnerability which exists in System.Data.SqlClient and Microsoft.Data.SqlClient libraries where a timeout occurring under high load can cause incorrect data to be returned as the result of an asynchronously executed query or command.	KB5020690	Applicable on Security Module devices.
2022-11 Security Only Update for .NET Framework 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 for x64 (KB5020680)	This security update addresses a vulnerability which exists in System.Data.SqlClient and Microsoft.Data.SqlClient libraries where a timeout occurring under high load can cause incorrect data to be returned as the result of an asynchronously executed query or command.	KB5020680	Applicable on Security Module devices.
2022-11 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 (KB5020629)	This security update addresses a vulnerability which exists in System.Data.SqlClient and Microsoft.Data.SqlClient libraries where a timeout occurring under high load can cause incorrect data to be returned as the result of an asynchronously executed query or command.	KB5020629	Applicable on Security Module devices.
2022-11 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5019964)	This security update includes quality improvements. When you install this KB: • It stops the start of daylight saving time in Jordan at the end of October 2022. The Jordan time zone will permanently shift to the UTC + 3 time zone. • It address an issue that affects the Microsoft Azure Active Directory (AAD) Application Proxy connector. It cannot retrieve a Kerberos ticket on behalf of the user. The error message is, "The handle specified is invalid (0x80090301)."	KB5019964	Applicable on Security Module devices.

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

bd.com

Security Patches: BD Pyxis™ IV Prep

November 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for November 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 - v5.107	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
2022-11 Security Only Update for .NET Framework 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.	KB5020680	Applicable on Cato

2022-11 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.	KB5020690	Applicable on Cato
2022-11 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	KB5020010	Applicable on Cato
2022-11 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.	KB5020023	Applicable on Cato
2022-11 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update.	KB5019958	Applicable on Cato
2022-11 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.	KB5019964	Applicable on Cato

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

bd.com

Security Patches: BD Pyxis Connect

November 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for November 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
2022-11 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5019964)	This security update includes quality improvements. When you install this KB: • It addresses an issue that affects Distributed Component Object Model (DCOM) authentication hardening. We will automatically raise the authentication level for all non-anonymous activation requests from DCOM clients to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY. This occurs if the authentication level is below Packet Integrity. • It stops the start of daylight-saving time in Jordan at the end of October 2022. The Jordan time zone will permanently shift to the UTC + 3 time zone. • It addresses an issue that affects the Microsoft Azure Active Directory (AAD) Application Proxy connector. It cannot retrieve a Kerberos ticket on behalf of the user. The error message is, "The handle specified is invalid (0x80090301)." • It addresses an issue that affects the Forest Trust creation process. It fails to add the Domain Name System (DNS) name suffixes to the trust information attributes. This occurs after you install the January 11, 2022, or later updates. • It addresses an issue that affects a domain controller (DC). The DC writes Key Distribution Center (KDC) event 21 in the System event log. This occurs when the KDC successfully processes a Kerberos Public Key Cryptography for Initial Authentication (PKINIT) authentication request using a self-	KB5019964	N/A

	signed certificate for key trust scenarios. This includes Windows Hello for Business and Device Authentication. • It addresses an issue that affects the Microsoft Visual C++ Redistributable Runtime. It does not load into the Local Security Authority Server Service (LSASS) when you enable Protected Process Light (PPL). • It addresses security vulnerabilities in the Kerberos and Netlogon protocols.		
2022-11 Cumulative Update for .NET Framework 4.8 for Windows Server 2016 for x64 (KB5020614)	This security update addresses a vulnerability which exists in System.Data.SqlClient and Microsoft.Data.SqlClient libraries where a timeout occurring under high load can cause incorrect data to be returned as the result of an asynchronously executed query or command.	KB5020614	N/A
Windows Malicious Software Removal Tool x64 - v5.107 (KB890830)	Windows Malicious Software Removal Tool (MSRT) helps keep Windows computers free from prevalent malware. MSRT finds and removes threats and reverses the changes made by these threats. MSRT is generally released monthly as part of Windows Update or as a standalone tool.	KB890830	N/A
2022-11 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems (KB5019958)	This security update resolves vulnerabilities in Internet Explorer. This update applies to the following: • Internet Explorer 11 on Windows Server 2012 R2 • Internet Explorer 11 on Windows 8.1 • Internet Explorer 11 on Windows Server 2012 • Internet Explorer 11 on Windows Server 2008 R2 SP1 • Internet Explorer 11 on Windows 7 SP1	KB5019958	N/A

2022-11 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5020023)	This cumulative security update includes following improvements: • Addresses a Distributed Component Object Model (DCOM) authentication hardening issue to automatically raise authentication level for all non-anonymous activation requests from DCOM clients. This will occur if the authentication level is less than RPC_C_AUTHN_LEVEL_PKT_INTEGRITY. • Updates the daylight-saving time (DST) for Jordan to prevent moving the clock back 1 hour on October 28, 2022. Additionally, changes the display name of Jordan standard time from "(UTC+02:00) Amman" to "(UTC+03:00) Amman". • Addresses an issue where Microsoft Azure Active Directory (AAD) Application Proxy Connector cannot retrieve a Kerberos ticket on behalf of the user because of the following general API error: "The handle specified is invalid (0x80090301)." • Addresses an issue where, after installing the January 11, 2022 or later update, the Forest Trust creation process fails to populate the DNS name suffixes into the trust information attributes. • Addresses an issue where the Microsoft Visual C++ Redistributable Runtime does not load into the Local Security Authority Server Service (LSASS) when Protected Process Light (PPL) is enabled. • Addresses security vulnerabilities in the Kerberos and Netlogon protocols.	KB5020023	N/A
2022-11 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5020010)	This security-only update includes key changes for the following: • Updates the daylight-saving time (DST) for Jordan to prevent moving the clock back 1 hour on October 28, 2022. Additionally, changes the display name of Jordan standard time from "(UTC+02:00) Amman" to "(UTC+03:00) Amman". • Addresses an issue where, after installing the January 11, 2022 or later update, the Forest Trust creation process fails to populate the DNS name suffixes into the trust information attributes. • Addresses security vulnerabilities in the Kerberos and Netlogon protocols.	KB5020010	N/A

2022-11 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 (KB5020690)	This security update addresses a vulnerability which exists in System.Data.SqlClient and Microsoft.Data.SqlClient libraries where a timeout occurring under high load can cause incorrect data to be returned as the result of an asynchronously executed query or command.	KB5020690	N/A
2022-11 Security Only Update for .NET Framework 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 for x64 (KB5020680)	This security update addresses a vulnerability which exists in System.Data.SqlClient and Microsoft.Data.SqlClient libraries where a timeout occurring under high load can cause incorrect data to be returned as the result of an asynchronously executed query or command.	KB5020680	N/A
2022-11 Cumulative Update for Windows 10 Version 22H2 for x64-based Systems (KB5019959)	It addresses security issues for your Windows operating system.	KB5019959	N/A
2022-11 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2 (KB5020694)	This security update addresses a vulnerability which exists in System.Data.SqlClient and Microsoft.Data.SqlClient libraries where a timeout occurring under high load can cause incorrect data to be returned as the result of an asynchronously executed query or command.	KB5020694	N/A

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

bd.com

Security Patches: BD Pharmogistics

November 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for November 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.
2022-10 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	The following articles contain additional information about this update as it relates to individual product versions. 5016268 Description of the Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 (KB5016268) 5018523 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 (KB5018523)	KB5018549	N/A

	5018519 Description of the Security and Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 (KB5018519)		
2022-11 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5020023) Last Modified: 11/8/2022	Addresses a Distributed Component Object Model (DCOM) authentication hardening issue to automatically raise authentication level for all non-anonymous activation requests from DCOM clients. This will occur if the authentication level is less than RPC_C_AUTHN_LEVEL_PKT_INTEGRITY. Updates the daylight-saving time (DST) for Jordan to prevent moving the clock back 1 hour on October 28, 2022. Additionally, changes the display name of Jordan standard time from “(UTC+02:00) Amman” to “(UTC+03:00) Amman”. Addresses an issue where Microsoft Azure Active Directory (AAD) Application Proxy Connector cannot retrieve a Kerberos ticket on behalf of the user because of the following general API error: “The handle specified is invalid (0x80090301).”	KB5020023	N/A
2022-11 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 (KB5020690) Last Modified: 11/8/2022	The November 8, 2022 update for Windows 8.1, RT 8.1, and Windows Server 2012 R2 includes Security and Quality Rollup improvements. We recommend that you apply this update as part of your regular maintenance routines. Security Improvements This security update addresses a vulnerability which exists in System.Data.SqlClient and Microsoft.Data.SqlClient libraries where a timeout occurring under high load can cause incorrect data to be returned as the result of an asynchronously executed	KB5020690	N/A

	query or command. For more information please see CVE-2022-41064.		
2022-11 Security Only Update for .NET Framework 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2008 R2 for x64 (KB5020678) Last Modified: 11/8/2022	This security update addresses a vulnerability which exists in System.Data.SqlClient and Microsoft.Data.SqlClient libraries where a timeout occurring under high load can cause incorrect data to be returned as the result of an asynchronously executed query or command. For more information please see CVE-2022-41064.	KB5020678	N/A
2022-11 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 Server 2008 R2 for x64 (KB5020688) Last Modified: 11/8/2022	The November 8, 2022 update for Windows 7 SP1 and Windows Server 2008 R2 SP1 includes Security and Quality Rollup improvements. We recommend that you apply this update as part of your regular maintenance routines. Security Improvements This security update addresses a vulnerability which exists in System.Data.SqlClient and Microsoft.Data.SqlClient libraries where a timeout occurring under high load can cause incorrect data to be returned as the result of an asynchronously executed query or command. For more information please see CVE-2022-41064.	KB5020688	N/A

2022-11 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (KB5020000) Last Modified: 11/8/2022	This cumulative security update contains improvements that are part of update KB5017361 (released October 11, 2022) and includes key changes for the following: Addresses a Distributed Component Object Model (DCOM) authentication hardening issue to automatically raise authentication level for all non-anonymous activation requests from DCOM clients. This will occur if the authentication level is less than RPC_C_AUTHN_LEVEL_PKT_INTEGRITY. Updates the daylight-saving time (DST) for Jordan to prevent moving the clock back 1 hour on October 28, 2022. Additionally, changes the display name of Jordan standard time from “(UTC+02:00) Amman” to “(UTC+03:00) Amman”.	KB5020000	N/A
2022-11 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 21H2 for x64 (KB5020687) Last Modified: 11/8/2022	This article describes the Cumulative Update for 3.5, 4.8 and 4.8.1 for Windows 10 Version 21H2. Security Improvements This security update addresses a vulnerability which exists in System.Data.SqlClient and Microsoft.Data.SqlClient libraries where a timeout occurring under high load can cause incorrect data to be returned as the result of an asynchronously executed query or command. For more information please see CVE-2022-41064.	KB5020687	N/A
2022-11 Dynamic Cumulative Update for Windows 10 Version 21H2 for x64-based Systems (KB5019959) Last Modified: 11/8/2022	Windows 10 servicing stack update - 19042.2180, 19043.2180, 19044.2180, and 19045.2180 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.	KB5019959	N/A

2022-11 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5019964) Last Modified: 11/8/2022	This security update includes quality improvements. When you install this KB: It addresses an issue that affects Distributed Component Object Model (DCOM) authentication hardening. We will automatically raise the authentication level for all non-anonymous activation requests from DCOM clients to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY. This occurs if the authentication level is below Packet Integrity. It stops the start of daylight saving time in Jordan at the end of October 2022. The Jordan time zone will permanently shift to the UTC + 3 time zone. It address an issue that affects the Microsoft Azure Active Directory (AAD) Application Proxy connector. It cannot retrieve a Kerberos ticket on behalf of the user. The error message is, “The handle specified is invalid (0x80090301).”	KB5019964	N/A

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

bd.com

Security Patches: PARx

Nov 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for Nov 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 - v5.107	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
2022-11 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	This security update includes quality improvements. When you install this KB: It addresses an issue that affects Distributed Component Object Model (DCOM) authentication hardening. We will automatically raise the authentication level for all non-anonymous activation requests from DCOM clients to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY. This occurs if the authentication level is below Packet Integrity. It stops the start of daylight saving time in Jordan at the end of October 2022. The Jordan time zone will permanently shift to the UTC + 3 time zone. It address an issue that affects the Microsoft Azure Active Directory (AAD) Application Proxy connector. It cannot retrieve a Kerberos ticket on behalf of the	KB5019964	Applicable on ParX

user. The error message is, “The handle specified is invalid (0x80090301).”
It addresses an issue that affects the Forest Trust creation process. It fails to add the Domain Name System (DNS) name suffixes to the trust information attributes. This occurs after you install the January 11, 2022, or later updates.
It addresses an issue that affects a domain controller (DC). The DC writes Key Distribution Center (KDC) event 21 in the System event log. This occurs when the KDC successfully processes a Kerberos Public Key Cryptography for Initial Authentication (PKINIT) authentication request using a self-signed certificate for key trust scenarios. This includes Windows Hello for Business and Device Authentication.
It addresses an issue that affects the Microsoft Visual C++ Redistributable Runtime. It does not load into the Local Security Authority Server Service (LSASS) when you enable Protected Process Light (PPL).
It addresses security vulnerabilities in the Kerberos and Netlogon protocols as outlined in CVE-2022-38023, CVE-2022-37966, and CVE-2022-37967. For deployment guidance, see the following:
KB5020805: How to manage the Kerberos Protocol changes related to CVE-2022-37967
KB5021130: How to manage Netlogon Protocol changes related to CVE-2022-38023
KB5021131: How to manage the Kerberos Protocol changes related to CVE-2022-37966
If you installed earlier updates, only the new updates contained in this package will be downloaded and installed on your device.
For more information about security vulnerabilities, please refer to the new Security Update Guide website and the November 2022 Security Updates.

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

Security Patches: TIM

Nov 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for Nov 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
2022-11 Cumulative Update for Windows Server 2016 for x64-based Systems	This security update includes quality improvements. When you install this KB: It addresses an issue that affects Distributed Component Object Model (DCOM) authentication hardening. We will automatically raise the authentication level for all non-anonymous activation requests from DCOM clients to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY. This occurs if the authentication level is below Packet Integrity. It stops the start of daylight saving time in Jordan at the end of October 2022. The Jordan time zone will permanently shift to the UTC + 3 time zone. It address an issue that affects the Microsoft Azure Active Directory (AAD) Application Proxy connector. It cannot retrieve a Kerberos ticket on behalf of the user. The error message is, "The handle specified is invalid (0x80090301)." It addresses an issue that affects the Forest Trust creation process. It fails to add the Domain Name System (DNS) name suffixes to the trust information attributes. This occurs after you install the January 11, 2022, or later updates.	KB5019964	Applicable on TIM.

	It addresses an issue that affects a domain controller (DC). The DC writes Key Distribution Center (KDC) event 21 in the System event log. This occurs when the KDC successfully processes a Kerberos Public Key Cryptography for Initial Authentication (PKINIT) authentication request using a self-signed certificate for key trust scenarios. This includes Windows Hello for Business and Device Authentication. It addresses an issue that affects the Microsoft Visual C++ Redistributable Runtime. It does not load into the Local Security Authority Server Service (LSASS) when you enable Protected Process Light (PPL). It addresses security vulnerabilities in the Kerberos and Netlogon protocols as outlined in CVE-2022-38023, CVE-2022-37966, and CVE-2022-37967. For deployment guidance, see the following: KB5020805: How to manage the Kerberos Protocol changes related to CVE-2022-37967 KB5021130: How to manage Netlogon Protocol changes related to CVE-2022-38023 KB5021131: How to manage the Kerberos Protocol changes related to CVE-2022-37966 If you installed earlier updates, only the new updates contained in this package will be downloaded and installed on your device.		
Windows Malicious Software Removal Tool x64 - v5.107	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	KB890830	Applicable on TIM.

Windows Server 2012

Windows Server 2008 R2

Windows 7

Windows Server 2008

Microsoft releases the MSRT on a monthly cadence as part of Windows Update or as a standalone tool. Use this tool to find and remove specific prevalent threats and reverse the changes they have made (see covered malware families). For comprehensive malware detection and removal, consider using Windows Defender Offline or Microsoft Safety Scanner.

This article contains information about how the tool differs from an antivirus or antimalware product, how you can download and run the tool, what happens when the tool finds malware, and tool release information. It also includes information for the administrators and advanced users, including information about supported command-line switches.

Notes:

In compliance with the Microsoft Support Lifecycle policy, the MSRT is no longer supported on Windows Vista or earlier platforms. For more information, go to Microsoft Support Lifecycle.

If you are having problems in regards to an MSRT update within Windows Update, see Troubleshooting problems updating Windows 10.

2022-11 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	The November 8, 2022 update for Windows 8.1, RT 8.1, and Windows Server 2012 R2 includes Security and Quality Rollup improvements. We recommend that you apply this update as part of your regular maintenance routines. Security Improvements This security update addresses a vulnerability which exists in System.Data.SqlClient and Microsoft.Data.SqlClient libraries where a timeout occurring under high load can cause incorrect data to be returned as the result of an asynchronously executed query or command. For more information please see CVE-2022-41064. Quality and Reliability 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..	KB5020690	Applicable on TIM.
2022-11 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems	This cumulative security update includes improvements that are part of update KB5018474 (released October 11, 2022) and includes key changes for the following: Addresses a Distributed Component Object Model (DCOM) authentication hardening issue to automatically raise authentication level for all non-anonymous activation requests from DCOM clients. This will occur if the authentication level is less than RPC_C_AUTHN_LEVEL_PKT_INTEGRITY. Updates the daylight-saving time (DST) for Jordan to prevent moving the clock back 1 hour on October 28, 2022. Additionally, changes the display name of Jordan standard time from “(UTC+02:00) Amman” to “(UTC+03:00) Amman”. Addresses an issue where Microsoft Azure Active Directory (AAD) Application Proxy Connector cannot retrieve a Kerberos ticket on behalf of the user because of the following general API error: “The handle specified is invalid (0x80090301).”	KB5020023	Applicable on TIM.

	Addresses an issue where, after installing the January 11, 2022 or later update, the Forest Trust creation process fails to populate the DNS name suffixes into the trust information attributes. Addresses an issue where the Microsoft Visual C++ Redistributable Runtime does not load into the Local Security Authority Server Service (LSASS) when Protected Process Light (PPL) is enabled. Addresses security vulnerabilities in the Kerberos and Netlogon protocols as outlined in CVE-2022-38023, CVE-2022-37966, and CVE-2022-37967. For deployment guidance, see the following articles: KB5020805: How to manage the Kerberos protocol changes related to CVE-2022-37967 KB5021130: How to manage the Netlogon protocol changes related to CVE-2022-38023 KB5021131: How to manage the Kerberos protocol changes related to CVE-2022-37966 For more information about the resolved security vulnerabilities, please refer to the Deployments | Security Update Guide and the November 2022 Security Updates. For more information about the resolved security vulnerabilities, please refer to the Deployments | Security Update Guide and the November 2022 Security Updates.		
2022-11 Security Only Update for .NET Framework 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 for x64	This security update addresses a vulnerability which exists in System.Data.SqlClient and Microsoft.Data.SqlClient libraries where a timeout occurring under high load can cause incorrect data to be returned as the result of an asynchronously executed query or command. For more information please see CVE-2022-41064.	KB5020680	Applicable on TIM.

2022-11 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems	This security-only update includes key changes for the following: Updates the daylight-saving time (DST) for Jordan to prevent moving the clock back 1 hour on October 28, 2022. Additionally, changes the display name of Jordan standard time from “(UTC+02:00) Amman” to “(UTC+03:00) Amman”. Addresses an issue where, after installing the January 11, 2022 or later update, the Forest Trust creation process fails to populate the DNS name suffixes into the trust information attributes. Addresses security vulnerabilities in the Kerberos and Netlogon protocols as outlined in CVE-2022-38023, CVE-2022-37966, and CVE-2022-37967. For deployment guidance, see the following articles: KB5020805: How to manage the Kerberos protocol changes related to CVE-2022-37967 KB5021130: How to manage the Netlogon protocol changes related to CVE-2022-38023 KB5021131: How to manage the Kerberos protocol changes related to CVE-2022-37966 For more information about the resolved security vulnerabilities, please refer to the Deployments | Security Update Guide and the November 2022 Security Updates. For more information about the resolved security vulnerabilities, please refer to the Deployments | Security Update Guide and the November 2022 Security Updates.	KB5020010	Applicable on TIM.
2022-11 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems	This security update resolves vulnerabilities in Internet Explorer. To learn more about these vulnerabilities, see Deployments | Security Update Guide. Additionally, see the following articles for more information about cumulative updates: Windows Server 2008 SP2 update history Windows 7 SP1 and Windows Server 2008 R2 SP1 update history Windows Server 2012 update history Windows 8.1 and Windows Server 2012 R2 update history	KB5019958	Applicable on TIM.

2022-11 Cumulative Update for .NET Framework 4.8 for Windows Server 2016 for x64	This security update addresses a vulnerability which exists in System.Data.SqlClient and Microsoft.Data.SqlClient libraries where a timeout occurring under high load can cause incorrect data to be returned as the result of an asynchronously executed query or command. For more information please see CVE-2022-41064. Quality and Reliability Improvements WPF1 - Addresses an issue where a FailFast crash could occur when using WebBrowser.NavigateToString. - Addresses an ArgumentOutOfRangeException that can arise when calling ListBox.ScrollIntoView while there are pending changes to the visual tree that will change or clear the underlying ItemsCollection. - Addresses an ArgumentException "Width and Height must be non-negative" that can arise in an ItemsControl with grouping enabled, custom margins on the GroupItems, collapse/expand of GroupItems enabled, and run in high-DPI.	KB5020614	Applicable on TIM.

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

bd.com

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

November 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for November 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
2022-11 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.	KB5019966	Applicable on PAS device.
2022-11 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.	KB5020685	Applicable on PAS device.

Windows Malicious Software Removal Tool x64 - v5.107	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.
2022-11 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	KB5019964	Applicable on PAS device.
2022-11 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5019958	Applicable on PAS device.

2022-11 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.	KB5020013	Applicable on PAS device.
2022-11 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.	KB5020000	Applicable on PAS device.

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

bd.com

Security Patches:
BD Pyxis™ CIISafe ES

November 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for November 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
2022-11 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.	KB5019966	Applicable on CIISafe device.
2022-11 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 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.	KB5020685	Applicable on CIISafe device.

Windows Malicious Software Removal Tool x64 - v5.106	**After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.**	KB890830	**Applicable on CIISafe device.**
2022-11 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.**	KB5019959	**Applicable on CIISafe device.**

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

bd.com

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

November 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for November 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
2022-11 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 a ssociated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5020000	Applicable on Medstn ES device.
2022-11 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.	KB5020614	Applicable on Medstn ES device.

Windows Malicious Software Removal Tool x64 - v5.107	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.
2022-11 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.	KB5019964	Applicable on Medstn ES device.

2022-11 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.	KB5020013	Applicable on Medstn ES device.
2022-11 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5019958	Applicable on Medstn Es device.
2022-11 Cumulative Update for Windows 10 Version 1809 for ARM64-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.	KB5019966	Applicable on Medstn Es device.
2022-11 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.	KB5020685	Applicable on Medstn Es device.

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

bd.com

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

November 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for November 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
2022-11 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5019958	Applicable on MedES Server.
2022-11 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.	KB5020023	Applicable on MedES Server.

Windows Malicious Software Removal Tool x64 – v5.107	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.
2022-11 Cumulative Update for Windows Server 2016 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.	KB5019964	Applicable on MedES Server.
2022-11 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.	KB5020010	Applicable on MedES Server.

2022-11 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.	KB5020690	Applicable on MedES Server.
2022-11 Security Only Update for .NET Framework 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.	KB5020680	Applicable on MedES Server.

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

bd.com

Security Patches: BD Pyxis™ Supply

November 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for November 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
2022-11 Security Only Update for .NET Framework 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 for x64 (KB5020680)	This security update addresses a vulnerability which exists in System.Data.SqlClient and Microsoft.Data.SqlClient libraries where a timeout occurring under high load can cause incorrect data to be returned as the result of an asynchronously executed query or command. For more information please see CVE-2022-41064.	KB5020680	Applicable on Supply.
2022-11 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 (KB5020690)	This security update addresses a vulnerability which exists in System.Data.SqlClient and Microsoft.Data.SqlClient libraries where a timeout occurring under high load can cause incorrect data to be returned as the result of an asynchronously executed query or command. For more information please see CVE-2022-41064.	KB5020690	Applicable on Supply.
2022-11 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5020010)	This security-only update includes key changes for the following: • Updates the daylight-saving time (DST) for Jordan to prevent moving the clock back 1 hour on October 28, 2022. Additionally, changes the display name of Jordan standard time from "(UTC+02:00) Amman" to "(UTC+03:00) Amman". • Addresses an issue where, after installing the January 11, 2022 or later update, the Forest Trust creation process fails to populate the DNS name suffixes into the trust information attributes. • Addresses security vulnerabilities in the Kerberos and Netlogon protocols as outlined	KB5020010	Applicable on Supply.

	in CVE-2022-38023, CVE-2022-37966, and CVE-2022-37967. For deployment guidance, see the following articles: • KB5020805: How to manage the Kerberos protocol changes related to CVE-2022-37967 • KB5021130: How to manage the Netlogon protocol changes related to CVE-2022-38023 • KB5021131: How to manage the Kerberos protocol changes related to CVE-2022-37966		
2022-11 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5020023)	This cumulative security update includes improvements that are part of update KB5018474 (released October 11, 2022) and includes key changes for the following: • Addresses a Distributed Component Object Model (DCOM) authentication hardening issue to automatically raise authentication level for all non-anonymous activation requests from DCOM clients. This will occur if the authentication level is less than RPC_C_AUTHN_LEVEL_PKT_INTEGRITY. • Updates the daylight-saving time (DST) for Jordan to prevent moving the clock back 1 hour on October 28, 2022. Additionally, changes the display name of Jordan standard time from "(UTC+02:00) Amman" to "(UTC+03:00) Amman". • Addresses an issue where Microsoft Azure Active Directory (AAD) Application Proxy Connector cannot retrieve a Kerberos ticket on behalf of the user because of the following general API error: "The handle specified is invalid (0x80090301)." • Addresses an issue where, after installing the January 11, 2022 or later update, the Forest Trust creation process fails to populate the DNS name suffixes into the trust information attributes. • Addresses an issue where the Microsoft Visual C++ Redistributable Runtime does not load into the Local Security Authority Server Service (LSASS) when Protected Process Light (PPL) is enabled. • Addresses security vulnerabilities in the Kerberos and Netlogon protocols as outlined in CVE-2022-38023, CVE-2022-37966, and CVE-2022-37967. For deployment guidance, see the following articles: • KB5020805: How to manage the Kerberos protocol changes related to CVE-2022-37967 • KB5021130: How to manage the Netlogon protocol changes related to CVE-2022-38023 • KB5021131: How to manage the Kerberos protocol changes related to CVE-2022-37966	KB5020023	Applicable on Supply.

2022-11 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems (KB5019958)	This security update resolves vulnerabilities in Internet Explorer. To learn more about these vulnerabilities, see Deployments I Security Update Guide.	KB5019958	Applicable on Supply.
2022-11 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5019964)	This security update includes quality improvements. When you install this KB: • It addresses an issue that affects Distributed Component Object Model (DCOM) authentication hardening. We will automatically raise the authentication level for all non-anonymous activation requests from DCOM clients to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY. This occurs if the authentication level is below Packet Integrity. • It stops the start of daylight saving time in Jordan at the end of October 2022. The Jordan time zone will permanently shift to the UTC + 3 time zone. • It address an issue that affects the Microsoft Azure Active Directory (AAD) Application Proxy connector. It cannot retrieve a Kerberos ticket on behalf of the user. The error message is, “The handle specified is invalid (0x80090301).” • It addresses an issue that affects the Forest Trust creation process. It fails to add the Domain Name System (DNS) name suffixes to the trust information attributes. This occurs after you install the January 11, 2022, or later updates. • It addresses an issue that affects a domain controller (DC). The DC writes Key Distribution Center (KDC) event 21 in the System event log. This occurs when the KDC successfully processes a Kerberos Public Key Cryptography for Initial Authentication (PKINIT) authentication request using a self-signed certificate for key trust scenarios. This includes Windows Hello for Business and Device Authentication. • It addresses an issue that affects the Microsoft Visual C++ Redistributable Runtime. It does not load into the Local Security Authority Server Service (LSASS) when you enable Protected Process Light (PPL). • It addresses security vulnerabilities in the Kerberos and Netlogon protocols as outlined in CVE-2022-38023, CVE-2022-37966, and CVE-2022-37967. For deployment guidance, see the following: • KB5020805: How to manage the Kerberos Protocol changes related to CVE-2022-37967	KB5019964	Applicable on Supply.

	• KB5021130: How to manage Netlogon Protocol changes related to CVE-2022-38023 • KB5021131: How to manage the Kerberos Protocol changes related to CVE-2022-37966		
2022-11 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 (KB5020685)	This security update addresses a vulnerability which exists in System.Data.SqlClient and Microsoft.Data.SqlClient libraries where a timeout occurring under high load can cause incorrect data to be returned as the result of an asynchronously executed query or command. For more information please see CVE-2022-41064.	KB5020685	Applicable on Supply.
2022-11 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10 Version 1809 for x64 (KB5020685)	This security update addresses a vulnerability which exists in System.Data.SqlClient and Microsoft.Data.SqlClient libraries where a timeout occurring under high load can cause incorrect data to be returned as the result of an asynchronously executed query or command. For more information please see CVE-2022-41064.	KB5020685	Applicable on Supply.
2022-11 Cumulative Update for Windows Server 2019 for x64-based Systems (KB5019966)	This security update includes improvements. When you install this KB: • New! It makes Microsoft compliant with US Government (USG) version 6 revision 1 (USGv6-r1). • It addresses an issue that affects Distributed Component Object Model (DCOM) authentication hardening. It automatically raises the authentication level for all non-anonymous activation requests from DCOM clients to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY. This occurs if the authentication level is below Packet Integrity. • It addresses a DCOM issue that affects the Remote Procedure Call Service (rpcss.exe). It raises the authentication level to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY instead of RPC_C_AUTHN_LEVEL_CONNECT if RPC_C_AUTHN_LEVEL_NONE is specified. • It stops the start of daylight saving time in Jordan at the end of October 2022. The Jordan time zone will permanently shift to the UTC + 3 time zone. • It address an issue that affects the Microsoft Azure Active Directory (AAD) Application Proxy connector. It cannot retrieve a Kerberos ticket on behalf of the user. The error message is, “The handle specified is invalid (0x80090301).” • It addresses an issue that affects the font of three Chinese characters. When you format	KB5019966	Applicable on Supply.

these characters as bold, the width size is wrong.
- It updates the Windows kernel vulnerable driver blocklist that is in the DriverSiPolicy.p7b file. This update also ensures that the blocklist is the same across Windows 10 and Windows 11. For more information, see KB5020779.
- It addresses an issue that affects focus order. This issue occurs when you tab from the password field on a credentials page.
- It addresses an issue that affects the Forest Trust creation process. It fails to add the Domain Name System (DNS) name suffixes to the trust information attributes. This occurs after you install the January 11, 2022, or later updates.
- It addresses a timing condition in Remote Desktop. It causes a device to stop working during the licensing process.
- It addresses an issue that affects Server Manager. It might reset the wrong disk when several disks have the same UniqueId. For more information, see KB5018898.
- It addresses an issue that causes the Host Networking Service (HNS) to stop working. This leads to traffic interruptions. For Windows Server 2019, this change is disabled by default. To turn it on requires a registry key. You can request this key from Microsoft through your Technical Account Manager (TAM). For Windows Server 2022, this change is enabled by default. No additional action is required after the system is updated.
- It addresses an issue that might occur when you enable deduplication. The issue might cause a deadlock.
- It addresses security vulnerabilities in the Kerberos and Netlogon protocols as outlined in CVE-2022-38023, CVE-2022-37966, and CVE-2022-37967. For deployment guidance, see the following:
- KB5020805: How to manage the Kerberos Protocol changes related to CVE-2022-37967
- KB5021130: How to manage Netlogon Protocol changes related to CVE-2022-38023
- KB5021131: How to manage the Kerberos Protocol changes related to CVE-2022-37966

2022-11 Cumulative Update for Windows Server 2019 for x64-based Systems (KB5019966)	This security update includes improvements. When you install this KB: • New! It makes Microsoft compliant with US Government (USG) version 6 revision 1 (USGv6-r1). • It addresses an issue that affects Distributed Component Object Model (DCOM) authentication hardening. It automatically raises the authentication level for all non-anonymous activation requests from DCOM clients to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY. This occurs if the authentication level is below Packet Integrity. • It addresses a DCOM issue that affects the Remote Procedure Call Service (rpcss.exe). It raises the authentication level to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY instead of RPC_C_AUTHN_LEVEL_CONNECT if RPC_C_AUTHN_LEVEL_NONE is specified. • It stops the start of daylight saving time in Jordan at the end of October 2022. The Jordan time zone will permanently shift to the UTC + 3 time zone. • It address an issue that affects the Microsoft Azure Active Directory (AAD) Application Proxy connector. It cannot retrieve a Kerberos ticket on behalf of the user. The error message is, “The handle specified is invalid (0x80090301).” • It addresses an issue that affects the font of three Chinese characters. When you format these characters as bold, the width size is wrong. • It updates the Windows kernel vulnerable driver blocklist that is in the DriverSiPolicy.p7b file. This update also ensures that the blocklist is the same across Windows 10 and Windows 11. For more information, see KB5020779. • It addresses an issue that affects focus order. This issue occurs when you tab from the password field on a credentials page. • It addresses an issue that affects the Forest Trust creation process. It fails to add the Domain Name System (DNS) name suffixes to the trust information attributes. This occurs after you install the January 11, 2022, or later updates. • It addresses a timing condition in Remote Desktop. It causes a device to stop working during the licensing process. • It addresses an issue that affects Server Manager. It might reset the wrong disk when several disks have the same UniqueId. For more information, see KB5018898. • It addresses an issue that causes the Host Networking Service (HNS) to stop working.	KB5019966	Applicable on Supply.

	This leads to traffic interruptions. For Windows Server 2019, this change is disabled by default. To turn it on requires a registry key. You can request this key from Microsoft through your Technical Account Manager (TAM). For Windows Server 2022, this change is enabled by default. No additional action is required after the system is updated. • It addresses an issue that might occur when you enable deduplication. The issue might cause a deadlock. • It addresses security vulnerabilities in the Kerberos and Netlogon protocols as outlined in CVE-2022-38023, CVE-2022-37966, and CVE-2022-37967. For deployment guidance, see the following: • KB5020805: How to manage the Kerberos Protocol changes related to CVE-2022-37967 • KB5021130: How to manage Netlogon Protocol changes related to CVE-2022-38023 • KB5021131: How to manage the Kerberos Protocol changes related to CVE-2022-37966		
Windows Malicious Software Removal Tool x64 - v5.107	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