Security Patches:
BD Pyxis™ Anesthesia System 3500

August 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for August 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
2022-08 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems.	This cumulative security update contains improvements that are part of update KB5015861 (released July 12, 2022) and includes new improvements for the following issues: Addresses an issue in which Speech and Network troubleshooters will not start. Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016676	Applicable on 3500 Anesthesia System and MS3500 Station

2022-08 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This security-only update includes new improvements for the following issue: Addresses an issue in which Speech and Network troubleshooters will not start. Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016679	Applicable on 3500 Anesthesia System and MS3500 Station
2022-08 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems.	This security update resolves vulnerabilities in Internet Explorer.	KB5016618	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

August 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for August 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 - v5.104	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS4000 Console, Anesthesia System and Station
2022-08 Cumulative Update for Windows 10 Version 1607 for x64-based Systems.	This security update includes quality improvements. Key changes include: Addresses an issue that prevents certain troubleshooting tools from opening. Addresses an issue that prevents the Key Distribution Center (KDC) Proxy from properly receiving Kerberos tickets for Key Trust Windows Hello for Business credentials. Addresses an issue that causes the KDC code to incorrectly return the error message "KDC_ERR_TGT_REVOKED" during domain controller shutdown. Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016622	Applicable on Anesthesia System and MS4000

2022-08 Servicing Stack Update for Windows 10 Version 1607 for x64-based Systems.	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.	KB5017095	Applicable on Anesthesia System and MS4000
2022-08 Security Update for Windows 10 Version 1607 for x64-based Systems.	his 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 Anesthesia System and MS4000
2022-08 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems.	This cumulative security update contains improvements that are part of update KB5015861 (released July 12, 2022) and includes new improvements for the following issues: Addresses an issue in which Speech and Network troubleshooters will not start. Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016676	Applicable on Anesthesia System and Station
2022-08 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems.	This security-only update includes new improvements for the following issue: Addresses an issue in which Speech and Network troubleshooters will not start. Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and scanners that use smart cards	KB5016679	Applicable on Anesthesia System and Station

	for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.		
2022-08 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems.	This security update resolves vulnerabilities in Internet Explorer.	KB5016618	Applicable on Anesthesia System and Station

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

bd.com

Security Patches: BD Pyxis CIISafe

August 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for August 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
2022-08 Security Monthly Quality Rollup 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.	KB5016676	Applicable to CIISafe device.
2022-08 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.	KB5016622	Applicable to CIISafe device.

2022-08 Servicing Stack Update for Windows 10 Version 1607 for x86-based System.	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.	KB5017095	Applicable to CIISafe device.

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

bd.com

Security Patches:
BD Pyxis™ MedStation™ 3500

August 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for August 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
2022-08 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems.	This security-only update includes new improvements for the following issue: Addresses an issue in which Speech and Network troubleshooters will not start. Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016679	Applicable on 3500 Anesthesia System and MS3500 Station
2022-08 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems.	This cumulative security update contains improvements that are part of update KB5015861 (released July 12, 2022) and includes new improvements for the following issues: Addresses an issue in which Speech and Network troubleshooters will not start. Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a	KB5016676	Applicable on 3500 Anesthesia System and MS3500 Station

	hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.		
Windows Malicious Software Removal Tool - v5.104	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS3500 and MS 4000 Console
2022-08 Security Only Quality Update for Windows Server 2008 for x86-based Systems.	This security-only update includes new improvements for the following issue: Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016686	Applicable on MS3500 and MS 4000 Console
2022-08 Security Monthly Quality Rollup for Windows Server 2008 for x86-based Systems.	This cumulative security update contains improvements that are part of update KB5015866 (released July 12, 2022) and includes new improvements for the following issue: Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016669	Applicable on MS3500 and MS 4000 Console

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

bd.com

Security Patches:
BD Pyxis™ MedStation™ 4000

August 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for August 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 - v5.104	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS4000 Console, Anesthesia System and Station
2022-08 Cumulative Update for Windows Server 2016 for x64-based Systems.	This security update includes quality improvements. Key changes include: Addresses an issue that prevents certain troubleshooting tools from opening. Addresses an issue that prevents the Key Distribution Center (KDC) Proxy from properly receiving Kerberos tickets for Key Trust Windows Hello for Business credentials. Addresses an issue that causes the KDC code to incorrectly return the error message "KDC_ERR_TGT_REVOKED" during domain controller shutdown. Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016622	Applicable on MS4000 Console

2022-08 Security Update for Windows Server 2016 for x64-based Systems.	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 MS4000 Console
2022-08 Servicing Stack Update for Windows Server 2016 for x64-based Systems.	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.	KB5017095	Applicable on MS4000 Console
2022-08 Cumulative Update for Windows 10 Version 1607 for x64-based Systems.	This security update includes quality improvements. Key changes include: Addresses an issue that prevents certain troubleshooting tools from opening. Addresses an issue that prevents the Key Distribution Center (KDC) Proxy from properly receiving Kerberos tickets for Key Trust Windows Hello for Business credentials. Addresses an issue that causes the KDC code to incorrectly return the error message “KDC_ERR_TGT_REVOKED” during domain controller shutdown. Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016622	Applicable on MS4000 and Anesthesia System
2022-08 Security Update for Windows 10 Version 1607 for x64-based Systems	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	KB5012170	Applicable on MS4000 and Anesthesia System

	vulnerability by adding the signatures of the known vulnerable UEFI modules to the DBX.		
2022-08 Servicing Stack Update for Windows 10 Version 1607 for x64-based Systems.	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.	KB5017095	Applicable on MS4000 and Anesthesia System
Windows Malicious Software Removal Tool - v5.104	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS4000 Console and MED3500 Console
2022-08 Security Only Quality Update for Windows Server 2008 for x86-based Systems.	This security-only update includes new improvements for the following issue: Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016686	Applicable on MS4000 Console and MED3500 Console
2022-08 Security Monthly Quality Rollup for Windows Server 2008 for x86-based Systems.	This cumulative security update contains improvements that are part of update KB5015866 (released July 12, 2022) and includes new improvements for the following issue: Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016669	Applicable on MS4000 Console and MED3500 Console

2022-08 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems.	This cumulative security update contains improvements that are part of update KB5015861 (released July 12, 2022) and includes new improvements for the following issues: Addresses an issue in which Speech and Network troubleshooters will not start. Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016676	Applicable on MS4000 and Anesthesia System
2022-08 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems.	This security-only update includes new improvements for the following issue: Addresses an issue in which Speech and Network troubleshooters will not start. Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016679	Applicable on MS4000 and Anesthesia System

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

bd.com

Security Patches: Security Module

August 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for August 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 - v5.104 (KB890830)	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	Applicable on Security Module devices.
2022-08 Security Update for Windows Server 2012 for x64-based Systems (KB5012170)	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.	KB5012170	Applicable on Security Module devices.
2022-08 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems (KB5016618)	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.	KB5016618	Applicable on Security Module devices.

2022-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5016681)	This cumulative security update includes improvements that are part of update KB5015874 (released July 12, 2022) and includes new improvements for the following issues: ▪ Addresses an issue in which Speech and Network troubleshooters will not start. ▪ Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. ▪ Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016681	Applicable on Security Module devices.
2022-08 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5016683)	This security-only update includes new improvements for the following issue: ▪ Addresses an issue in which Speech and Network troubleshooters will not start. ▪ Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. ▪ Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016683	Applicable on Security Module devices.
2022-08 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5016622)	This security update includes quality improvements. Key changes include: ▪ Addresses an issue that prevents certain troubleshooting tools from opening. ▪ Addresses an issue that prevents the Key Distribution Center (KDC) Proxy from properly receiving Kerberos tickets for Key Trust Windows Hello for Business credentials. ▪ Addresses an issue that causes the KDC code to incorrectly return the error message “KDC_ERR_TGT_REVOKED” during domain controller shutdown.	KB5016622	Applicable on Security Module devices.

	▪ Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. ▪ Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.		
2022-08 Servicing Stack Update for Windows Server 2016 for x64-based Systems (KB5017095)	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.	KB5017095	Applicable on Security Module devices.

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

bd.com

Security Patches: BD Pyxis™ IV Prep

August 2022

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

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.101	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	Applicable on Cato
2022-08 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.	KB5016622	Applicable on Cato

2022-08 Servicing Stack 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.	KB5017095	Applicable on Cato
2022-08 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	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.	KB5016740	Applicable on Cato
2022-08 Security 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.	KB5012170	Applicable on Cato
2022-08 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.	KB5016681	Applicable on Cato

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

bd.com

Security Patches: BD Pyxis Connect

August 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for August 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
2022-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems	Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016681	N/A
2022-08 Security Update for Windows Server 2012 R2**/2016** for x64-based Systems	This security update makes improvements to Secure Boot DBX for the supported Windows versions listed in the "Applies to" section.	KB5012170	N/A

Windows Malicious Software Removal Tool - v5.104(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
2022-08 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 I 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	KB5016618	N/A
2022-08 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems	This security-only update includes new improvements for the following issue: Addresses an issue in which Speech and Network troubleshooters will not start. Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will	KB5016683	N/A

	not exist after August 9, 2022. For more information about this change, see KB5005408.		
2022-08 Servicing Stack Update for Windows Server 2016 for x64-based Systems	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.	KB5017095	N/A
2022-08 Cumulative Update for Windows Server 2016 for x64-based Systems	This security update includes quality improvements. Key changes include: Addresses an issue that prevents certain troubleshooting tools from opening. Addresses an issue that prevents the Key Distribution Center (KDC) Proxy from properly receiving Kerberos tickets for Key Trust Windows Hello for Business credentials. Addresses an issue that causes the KDC code to incorrectly return the error message “KDC_ERR_TGT_REVOKED” during domain controller shutdown.	KB5016622	N/A

2022-08 Security Update for Windows Server 2019 for x64-based Systems	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	N/A
Cumulative Update for Windows 10 Version 21H2 for x64-based Systems (KB5016616)	Addresses an issue that affects the printing of files you submit to a printer. Addresses a known issue that might prevent the Input Indicator and Language Bar from displaying in the notification area. This issue affects devices that have more than one language installed. Addresses security issues for your Windows operating system.	KB5016616	

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

bd.com

Security Patches: BD Pharmogistics

August 2022

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

2022-08 Security Update for Windows Server 2012 R2 for x64-based Systems (KB5012170) Last Modified: 8/9/2022	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 PLX, CII Safe and Infusion.
2022-08 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5016622) Last Modified: 8/9/2022	Addresses an issue that prevents certain troubleshooting tools from opening. Addresses security issues for your Windows operating system. Improvements This security update includes quality improvements. Key changes include: Addresses an issue that prevents certain troubleshooting tools from opening. Addresses an issue that prevents the Key Distribution Center (KDC) Proxy from properly receiving Kerberos tickets for Key Trust Windows Hello for Business credentials. Addresses an issue that causes the KDC code to incorrectly return the error message “KDC_ERR_TGT_REVOKED” during domain controller shutdown.	KB5016622	Applicable on PLX, CII Safe and Infusion.

2022-08 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems (KB5016618) Last Modified: 8/9/2022	This security update resolves vulnerabilities in Internet Explorer. To learn more about these vulnerabilities, see Deployments | Security Update Guide.	KB5016618	Applicable on PLX, CII Safe and Infusion.
2022-08 Security Update for Windows Server 2012 R2 for x64-based Systems (KB5012170) Last Modified: 8/9/2022	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 PLX, CII Safe and Infusion.

2022-08 Servicing Stack Update for Windows Server 2016 for x64-based Systems (KB5017095) Last Modified: 8/9/2022	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.	KB5017095	Applicable on PLX, CII Safe and Infusion.
2022-08 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5016683) Last Modified: 8/9/2022	This security-only update includes new improvements for the following issue: Addresses an issue in which Speech and Network troubleshooters will not start. Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service.	KB5016683	Applicable on PLX, CII Safe and Infusion.
2022-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5016681) Last Modified: 8/9/2022	This cumulative security update includes improvements that are part of update KB5015874 (released July 12, 2022) and includes new improvements for the following issues: Addresses an issue in which Speech and Network troubleshooters will not start. Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device	KB5016681	Applicable on PLX, CII Safe and Infusion.

	performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service.		
2022-08 Security Update for Windows 10 Version 20H2 for x64-based Systems (KB5012170) Last Modified: 8/9/2022	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 PLX, CII Safe and Infusion.

2022-08 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (KB5016676) Last Modified: 8/9/2022	This cumulative security update contains improvements that are part of update KB5015861 (released July 12, 2022) and includes new improvements for the following issues: Addresses an issue in which Speech and Network troubleshooters will not start. Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service.	KB5016676	Applicable on PLX, CII Safe and Infusion.
2022-08 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 (KB5016738) Last Modified: 8/9/2022	Security Improvements This security update addresses an issue where a local user opening a specially crafted file could cause a denial of service condition on an affected system. For more information please see CVE-2022-30130. Quality Improvements For a list of improvements that were released with this update, please see the article links in the Additional Information section of this article.	KB5016738	Applicable on PLX, CII Safe and Infusion.
2022-08 Cumulative Security Update for Internet Explorer 11 for Windows Server 2008 R2 for x64-based systems (KB5016618) Last Modified: 8/9/2022	This security update resolves vulnerabilities in Internet Explorer. To learn more about these vulnerabilities, see Deployments | Security Update Guide.	KB5016618	Applicable on PLX, CII Safe and Infusion.

2022-08 Security Only Quality Update for Windows Server 2008 R2 for x64-based Systems (KB5016679) Last Modified: 8/9/2022	This security-only update includes new improvements for the following issue: Addresses an issue in which Speech and Network troubleshooters will not start. Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service.	KB5016679	Applicable on PLX, CII Safe and Infusion.
2022-08 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (KB5016676) Last Modified: 8/9/2022	This cumulative security update contains improvements that are part of update KB5015861 (released July 12, 2022) and includes new improvements for the following issues: Addresses an issue in which Speech and Network troubleshooters will not start. Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service.	KB5016676	Applicable on PLX, CII Safe and Infusion.

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

bd.com

Security Patches: PARx

Aug 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for Aug 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
Security Update for Windows 10 Version 1607 for x64-based Systems	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.	KB4535680	Applicable to Parx

2021-01 Update for Windows 10 Version 1607 for x64-based Systems	This update is a standalone update that is targeted at Windows 10, version 1607 and Windows Server 2016. This update also includes Intel microcode updates that were already released for these operating systems at the time of release	KB4589210	Applicable to Parx
Update for Removal of Adobe Flash Player for Windows 10 Version 1607 for x64-based systems	This update removes Adobe Flash Player that is installed on any of the Windows operating systems	KB4577586	Applicable to Parx
Windows Malicious Software Removal Tool x64 - v5.104	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers that are running any of the following operating systems: Windows 10 Windows Server 2019 Windows Server 2016 Windows 8.1 Windows Server 2012 R2 Windows Server 2012	KB890830	Applicable to Parx

	Windows Server 2008 R2 Windows 7 Windows Server 2008		
2022-08 Servicing Stack Update for Windows 10 Version 1607 for x64-based Systems	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.	KB5017095	Applicable to Parx
2022-08 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	This security update includes quality improvements. Key changes include: Addresses an issue that prevents certain troubleshooting tools from opening. Addresses an issue that prevents the Key Distribution Center (KDC) Proxy from properly receiving Kerberos tickets for Key Trust Windows Hello for Business credentials. Addresses an issue that causes the KDC code to incorrectly return the error message “KDC_ERR_TGT_REVOKED” during domain controller shutdown.	KB5016622	Applicable to Parx

	Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service.		
2022-08 Security Update for Windows 10 Version 1607 for x64-based Systems	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 to Parx

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

Security Patches: TIM

Aug 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for Aug 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
2022-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems	This cumulative security update includes improvements that are part of update KB5015874 (released July 12, 2022) and includes new improvements for the following issues: Addresses an issue in which Speech and Network troubleshooters will not start. Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016681	Applicable on TIM.

2022-08 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems	This security-only update includes new improvements for the following issue: Addresses an issue in which Speech and Network troubleshooters will not start. Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016683	Applicable on TIM.
2022-08 Security Update for Windows Server 2012 R2 for x64-based Systems	This security update applies only to the following Windows versions: Windows Server 2012 Windows 8.1 and Windows Server 2012 R2 Windows 10, version 1507 Windows 10, version 1607 and Windows Server 2016 Windows 10, version 1809 and Windows Server 2019 Windows 10, version 20H2 Windows 10, version 21H1 Windows 10, version 21H2 Windows Server 2022 Windows 11, version 21H2 (original release)	**KB5012170**	Applicable on TIM.

	Azure Stack HCI, version 1809 Azure Stack Data Box, version 1809 (ASDB) Summary 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.		
Windows Malicious Software Removal Tool x64 - v5.104	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers that are running any of the following operating systems: Windows 10 Windows Server 2019 Windows Server 2016 Windows 8.1 Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2 Windows 7 Windows Server 2008 Microsoft releases the MSRT on a monthly cadence as part of Windows Update or as a standalone tool. Use this tool to find and remove specific prevalent threats and reverse the changes they have made (see covered malware families). For comprehensive malware detection and removal, consider using Windows Defender Offline or Microsoft Safety Scanner. This article contains information about how the tool differs from an antivirus or antimalware	KB890830	Applicable on TIM.

	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.		
2022-08 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 I 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	KB5016618	Applicable on TIM.
2022-08 Servicing Stack Update for Windows Server 2016 for x64-based Systems	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.	KB5017095	Applicable on TIM.
2022-08 Cumulative Update for Windows Server 2016 for x64-based Systems	This security update includes quality improvements. Key changes include: Addresses an issue that prevents certain troubleshooting tools from opening. Addresses an issue that prevents the Key Distribution Center (KDC) Proxy from properly receiving Kerberos tickets for Key Trust Windows Hello for Business credentials. Addresses an issue that causes the KDC code to incorrectly return the error message “KDC_ERR_TGT_REVOKED” during domain controller shutdown. Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows	KB5016622	Applicable on TIM.

	updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408. 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 August 2022 Security Updates.		
2022-08 Cumulative Update for .NET Framework 4.8 for Windows Server 2016 for x64	There are no new security improvements in this release. This update is cumulative and contains all previously released security improvements.	KB5016373	Applicable on TIM.

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

bd.com

Security Patches:
BD **Pyxis™ CIISafe ES.**

August 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for August 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 - v5.104	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 CII Safe ES.

2022-08 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.	KB5012170	Applicable on CII Safe ES.
2022-08 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.	KB5016623	Applicable on CII Safe ES.
2022-08 Security Update for Windows 10 Version 21H2 9 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.	**KB5012170**	Applicable on CII Safe ES.
2022-08 Cumulative Update for Windows 10 Version 21H2 for x64-based Systems	A 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 system.	KB5016616	Applicable on CII Safe ES.

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

bd.com

Security Patches:
BD Pyxis™ ES Server

August 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for August 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
2022-08 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.	KB5016623	Applicable on Server.
2022-08 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.	KB5012170	Applicable on Server.

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

bd.com

Security Patches: BD Pyxis™ Supply

August 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for August 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
2022-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5016681)	This cumulative security update includes improvements that are part of update KB5015874 (released July 12, 2022) and includes new improvements for the following issues: • Addresses an issue in which Speech and Network troubleshooters will not start. • Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. • Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016681	Applicable on Supply.

2022-08 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5016683)	This security-only update includes new improvements for the following issue: • Addresses an issue in which Speech and Network troubleshooters will not start. • Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. • Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016683	Applicable on Supply.
2022-08 Security Update for Windows Server 2012 R2 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.
2022-08 Security Update for Windows 10 Version 1809 for x-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.	KB5012170	Applicable on Supply.

	• 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.		
2022-08 Security Update for Windows Server 2019 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.
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.
2022-08 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems (KB5016618)	This security update resolves vulnerabilities in Internet Explorer.	KB5016618	Applicable on Supply.

2022-08 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems (KB5016679)	This security-only update includes new improvements for the following issue: • Addresses an issue in which Speech and Network troubleshooters will not start. • Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. • Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016679	Applicable on Supply.
2022-08 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems (KB5016676)	This cumulative security update contains improvements that are part of update KB5015861 (released July 12, 2022) and includes new improvements for the following issues: • Addresses an issue in which Speech and Network troubleshooters will not start. • Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. • Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016676	Applicable on Supply.

2022-08 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5016622)	This security update includes quality improvements. Key changes include: • Addresses an issue that prevents certain troubleshooting tools from opening. • Addresses an issue that prevents the Key Distribution Center (KDC) Proxy from properly receiving Kerberos tickets for Key Trust Windows Hello for Business credentials. • Addresses an issue that causes the KDC code to incorrectly return the error message "KDC_ERR_TGT_REVOKED" during domain controller shutdown. • Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. • Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016622	Applicable on Supply.
2022-08 Servicing Stack Update for Windows Server 2016 for x64-based Systems (KB5017095)	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.	KB5017095	Applicable on Supply.
2022-08 Cumulative Update for Windows Server 2019 for x64-based Systems (KB5016623)	This security update includes improvements that were a part of update KB5015880 (released July 21, 2022) and also addresses the following issues: • Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service.	KB5016623	Applicable on Supply.

2022-08 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB5016623)	This security update includes improvements that were a part of update KB5015880 (released July 21, 2022) and also addresses the following issues: • Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service.	KB5016623	Applicable on Supply.
2022-08 Security Monthly Quality Rollup for Windows Server 2008 for x86-based Systems (KB5016669)	This cumulative security update contains improvements that are part of update KB5015866 (released July 12, 2022) and includes new improvements for the following issue: • Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. • Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016669	Applicable on Supply.

2022-08 Security Only Quality Update for Windows Server 2008 for x86-based Systems (KB5016686)	This security-only update includes new improvements for the following issue: • Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. • Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016686	Applicable on Supply.
Windows Malicious Software Removal Tool x64 - v5.104	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

Security Patches:
BD Pyxis™ Anesthesia ES

August 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for August 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 al Tool x64 - v5.104	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on Med station device.
2022-08 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This security-only update includes new improvements for the following issue: • Addresses an issue in which Speech and Network troubleshooters will not start. • Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. • Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more	KB5016679	Applicable on Anesthesia station.

	information about this change, see KB5005408.		
2022-08 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems.	This security update resolves vulnerabilities in Internet Explorer.	KB5016618	Applicable on Anesthesia station.
2022-08 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems.	This cumulative security update contains improvements that are part of update KB5015861 (released July 12, 2022) and includes new improvements for the following issues: Addresses an issue in which Speech and Network troubleshooters will not start. Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016676	Applicable on Anesthesia station.
2022-08 Cumulative Update for Windows 10 Version 1607 for x64-based Systems.	This security update includes quality improvements. Key changes include: Addresses an issue that prevents certain troubleshooting tools from opening. Addresses an issue that prevents the Key Distribution Center (KDC) Proxy from properly receiving Kerberos tickets for Key Trust Windows Hello for Business credentials. Addresses an issue that causes the KDC code to incorrectly return the error message “KDC_ERR_TGT_REVOKED” during domain controller shutdown. Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and	KB5016622	Applicable on Anesthesia station.

	scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.		
2022-08 Servicing Stack Update for Windows 10 Version 1607 for x64-based Systems.	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.	KB5017095	Applicable on Anesthesia station.
2022-08 Security Update for Windows 10 Version 1607 for x64-based Systems.	his 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 Anesthesia station.
2022-08 Security Update for Windows 10 Version 1809 for x-64-based Systems	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 Anesthesia station.

2022-08 Cumulative Update for Windows 10 Version 1809 for x64-based Systems	This security update includes improvements that were a part of update KB5015880 (released July 21, 2022) and also addresses the following issues: • Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service.	KB5016623	Applicable on Anesthesia station.

2022-08 Security Update for Windows 10 Version 21H2 9 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.	KB5012170	Applicable on Anesthesia station.
2022-08 Cumulative Update for Windows 10 Version 21H2 for x64-based Systems	A 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 system.	KB5016616	Applicable on Anesthesia station.

2022-08 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.	KB5012170	Applicable on Anesthesia station.

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

bd.com

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

August 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for August 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 - v5.104	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on Med station.
2022-08 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems	This security update resolves vulnerabilities in Internet Explorer.	KB5016618	Applicable on Med station.

2022-08 Security Update for Windows Server 2012 R2 for x64-based Systems	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 Med station.
2022-08 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems	This security-only update includes new improvements for the following issue: • Addresses an issue in which Speech and Network troubleshooters will not start. • Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016683	Applicable on Med station.

2022-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems	This cumulative security update includes improvements that are part of update KB5015874 (released July 12, 2022) and includes new improvements for the following issues: • Addresses an issue in which Speech and Network troubleshooters will not start. • Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016681	Applicable on Med station.
2022-08 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This security-only update includes new improvements for the following issue: • Addresses an issue in which Speech and Network troubleshooters will not start. • Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. • Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016679	Applicable on Med station.

2022-08 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems.	This cumulative security update contains improvements that are part of update KB5015861 (released July 12, 2022) and includes new improvements for the following issues: Addresses an issue in which Speech and Network troubleshooters will not start. Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016676	Applicable on Med station.
2022-08 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	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.	KB5016740	Applicable on Med station.
2022-08 Cumulative Update for Windows 10 Version 1607 for x64-based Systems.	This security update includes quality improvements. Key changes include: Addresses an issue that prevents certain troubleshooting tools from opening. Addresses an issue that prevents the Key Distribution Center (KDC) Proxy from properly receiving Kerberos tickets for Key Trust Windows Hello for Business credentials. Addresses an issue that causes the KDC code to incorrectly return the error message “KDC_ERR_TGT_REVOKED” during domain controller shutdown. Addresses an issue that might cause the	KB5016622	Applicable on Med station.

	Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.		
2022-08 Servicing Stack Update for Windows 10 Version 1607 for x64-based Systems.	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.	KB5017095	Applicable on Med station.
2022-08 Security Update for Windows 10 Version 1607 for x64-based Systems.	his 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 Med station.
2022-08 Security Update for Windows Server 2016 for x64-based Systems	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 Med station.

2022-08 Cumulative Update for Windows Server 2016 for x64-based Systems	This security update includes quality improvements. Key changes include: • Addresses an issue that prevents certain troubleshooting tools from opening. • Addresses an issue that prevents the Key Distribution Center (KDC) Proxy from properly receiving Kerberos tickets for Key Trust Windows Hello for Business credentials. • Addresses an issue that causes the KDC code to incorrectly return the error message "KDC_ERR_TGT_REVOKED" during domain controller shutdown. • Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service. • Enforces a hardening change that requires printers and scanners that use smart cards for authentication to have firmware that complies with section 3.2.1 of RFC 4556. If they do not comply, Active Directory domain controllers will not authenticate them. Mitigations that allowed non-compliant devices to authenticate will not exist after August 9, 2022. For more information about this change, see KB5005408.	KB5016622	Applicable on Med station.
2022-08 Servicing Stack Update for Windows Server 2016 for x64-based Systems	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.	KB5017095	Applicable on Med station.
2022-08 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.	KB5012170	Applicable on MedSTN device.

2022-08 Security Update for Windows 10 Version 1809 for x-64 based Systems	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 Med station.
2022-08 Cumulative Update for Windows 10 Version 1809 for x64-based Systems	This security update includes improvements that were a part of update KB5015880 (released July 21, 2022) and also addresses the following issues: • Addresses an issue that might cause the Local Security Authority Server Service (LSASS) to leak tokens. This issue affects devices that have installed Windows updates dated June 14, 2022 or later. This issue occurs when the device performs a specific form of service for user (S4U) in a non-Trusted Computing Base (TCB) Windows service that runs as Network Service.	KB5016623	Applicable on Med station.
2022-08 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems.	This security update resolves vulnerabilities in Internet Explorer.	KB5016618	Applicable on Med station.

2022-08 Security Update for Windows 10 Version 21H2 9 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.	KB5012170	Applicable on Med station.
2022-08 Cumulative Update for Windows 10 Version 21H2 for x64-based Systems	A 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 system.	KB5016616	Applicable on Med station.

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

bd.com