Security Patches:
BD Pyxis™ Anesthesia System 3500

July 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for July 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
2022-07 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems.	This cumulative security update contains improvements that are part of update KB5014748 (released June 14, 2022) and includes new improvements for the following issues: When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. NTLM authentication through an external trust is unsuccessful when serviced by a domain controller that has the January 11, 2022 or later Windows update installed. This issue occurs if the DC is in a non-root domain and does not hold the global catalog (GC) role. Impacted operations may log the following errors: The security database has not been started. The domain was in the wrong state to perform the security operation. 0xc00000dd (STATUS_INVALID_DOMAIN_STATE) Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects. Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic. Devices which connect to the server might not connect to the Internet, and servers can lose connection to the Internet after a client device connects.	KB5015861	Applicable on 3500 Anesthesia System and MS3500 Station

2022-07 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems.	This security-only update includes new improvements for the following issues: When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects. Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic. Devices which connect to the server might not connect to the Internet, and servers can lose connection to the Internet after a client device connects.	KB5015862	Applicable on 3500 Anesthesia System and MS3500 Station
2022-07 Servicing Stack Update for Windows Embedded Standard 7 for x86-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.	KB5016057	Applicable on 3500 Anesthesia System and MS3500 Station
2022-07 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems.	This security update resolves vulnerabilities in Internet Explorer.	KB5015805	Applicable on 3500 Anesthesia System and MS3500 Station

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

bd.com

BD and the BD Logo are trademarks of Becton, Dickinson and Company or its affiliates. © 2022 BD. All rights reserved.

Security Patches:
BD Pyxis™ Anesthesia System 4000

July 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for July 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 - v5.103	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS4000 Console, Anesthesia System and Station
2022-07 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	This security update includes quality improvements. Key changes include: Addresses an issue that causes searchindexer.exe to stop responding during a dismount operation in the Remote Desktop setup environment. Addresses an issue that redirects the PowerShell command output so that transcript logs do not contain any content. Transcript logs might contain decrypted passwords if you turn PowerShell logging on. Consequently, the transcript logs lose the decrypted passwords. Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the internet after a client device connects. Addresses an issue that prevents the use of Encrypted File System (EFS) files over a Web-based Distributed Authoring and Versioning (WebDAV) connection. Addresses an issue that causes Microsoft NTLM authentication using an external trust to fail. This issue occurs when a domain controller that contains the January 11, 2022 or later Windows update services the authentication request, is not in a root domain, and does not hold the Global Catalog role. The affected operations might log the following errors: The security database has not been started. The domain was in the wrong state to perform the security operation. 0xc00000dd	KB5015808	Applicable on Anesthesia System and MS4000

	(STATUS_INVALID_DOMAIN_STATE). Addresses an issue that causes the primary domain controller (PDC) of the root domain to generate warning and error events in the System log. This issue occurs when the PDC incorrectly tries to scan outgoing-only trusts. Addresses an issue that might damage BitLocker virtual machine-based (VM) system files if you expand the BitLocker partition while the VM is offline. Addresses a known issue that prevents Windows servers that use the Routing and Remote Access Service (RRAS) from correctly directing internet traffic. Devices that connect to the server might not connect to the internet, and servers might lose connection to the internet after a client device connects to them.		
2022-07 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.	KB5016058	Applicable on Anesthesia System and MS4000
2022-07 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5014748 (released June 14, 2022) and includes new improvements for the following issues: When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. NTLM authentication through an external trust is unsuccessful when serviced by a domain controller that has the January 11, 2022 or later Windows update installed. This issue occurs if the DC is in a non-root domain and does not hold the global catalog (GC) role. Impacted operations may log the following errors: The security database has not been started. The domain was in the wrong state to perform the security operation. 0xc00000dd (STATUS_INVALID_DOMAIN_STATE) Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects. Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic. Devices which connect to the server might not connect to the Internet, and servers can lose connection to the Internet after a client device connects.	KB5015861	Applicable on Anesthesia System and Station
2022-07 Cumulative Security Update for Internet Explorer 11 for Windows Embedded	This security update resolves vulnerabilities in Internet Explorer.	KB5015805	Applicable on Anesthesia

Restricted

Standard 7 for x86-based systems			System and Station
2022-07 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This security-only update includes new improvements for the following issues: When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects. Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic. Devices which connect to the server might not connect to the Internet, and servers can lose connection to the Internet after a client device connects.	KB5015862	Applicable on Anesthesia System and Station
2022-07 Servicing Stack Update for Windows Embedded Standard 7 for x86-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.	KB5016057	Applicable on Anesthesia System and Station

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

bd.com

BD and the BD Logo are trademarks of Becton, Dickinson and Company or its affiliates. © 2022 BD. All rights reserved.

Security Patches: BD Pyxis CIISafe

July 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for July 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
2022-07 Servicing Stack Update for Windows Embedded Standard 7 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.	KB5016057	Applicable to CIISafe device.
Windows Malicious Software Removal Tool x64 - v5.102	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 to CIISafe device.

2022-07 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x64-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5015861	Applicable to CIISafe device.
2022-07 Servicing Stack Update for Windows 10 Version 1607 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.	KB5016058	Applicable to CIISafe device.
2022-07 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5015808	Applicable to CIISafe device

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

bd.com

BD and the BD Logo are trademarks of Becton, Dickinson and Company or its affiliates. © 2022 BD. All rights reserved.

Security Patches:
BD Pyxis™ MedStation™ 3500

July 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for July 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
2022-07 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5014748 (released June 14, 2022) and includes new improvements for the following issues: When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. NTLM authentication through an external trust is unsuccessful when serviced by a domain controller that has the January 11, 2022 or later Windows update installed. This issue occurs if the DC is in a non-root domain and does not hold the global catalog (GC) role. Impacted operations may log the following errors: The security database has not been started. The domain was in the wrong state to perform the security operation. 0xc00000dd (STATUS_INVALID_DOMAIN_STATE) Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects. Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic. Devices which connect to the server might not connect to the Internet, and servers can lose connection to the Internet after a client device connects.	KB5015861	Applicable on 3500 Anesthesia System and MS3500 Station
2022-07 Security Only Quality Update for Windows Embedded	This security-only update includes new improvements for the following issues: When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful.	KB5015862	Applicable on 3500 Anesthesia System and MS3500 Station

Standard 7 for x86-based Systems.	Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects. Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic. Devices which connect to the server might not connect to the Internet, and servers can lose connection to the Internet after a client device connects.		
Windows Malicious Software Removal Tool - v5.103	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS3500 and MS 4000 Console
2022-07 Security Only Quality Update for Windows Server 2008 for x86-based Systems.	This security-only update includes new improvements for the following issues: When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects. Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic. Devices which connect to the server might not connect to the Internet, and servers can lose connection to the Internet after a client device connects.	KB5015870	Applicable on MS3500 and MS 4000 Console
2022-07 Security Monthly Quality Rollup for Windows Server 2008 for x86-based Systems.	This cumulative security update contains improvements that are part of update KB5014752 (released June 14, 2022) and includes new improvements for the following issues: When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. NTLM authentication through an external trust is unsuccessful when serviced by a domain controller that has the January 11, 2022 or later Windows update installed. This issue occurs if the DC is in a non-root domain and does not hold the global catalog (GC) role. Impacted operations may log the following errors:The security database has not been started. The domain was in the wrong state to perform the security operation. 0xc00000dd (STATUS_INVALID_DOMAIN_STATE) Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects. Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic. Devices which connect to the server	KB5015866	Applicable on MS3500 and MS 4000 Console

Restricted

	might not connect to the Internet, and servers can lose connection to the Internet after a client device connects.		
2022-07 Servicing Stack Update for Windows Server 2008 for x86-based Systems.	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) make sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.	KB5016129	Applicable on MS3500 and MS 4000 Console
2022-07 Servicing Stack Update for Windows Embedded Standard 7 for x86-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.	KB5016057	Applicable on 3500 Anesthesia System and MS3500 Station
2022-07 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems.	This security update resolves vulnerabilities in Internet Explorer.	KB5015805	Applicable on 3500 Anesthesia System and MS3500 Station

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

bd.com

BD and the BD Logo are trademarks of Becton, Dickinson and Company or its affiliates. © 2022 BD. All rights reserved.

Security Patches:
BD Pyxis™ MedStation™ 4000

July 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for July 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 - v5.103	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS4000 Console, Anesthesia System and Station
2022-07 Cumulative Update for Windows Server 2016 for x64-based Systems	This security update includes quality improvements. Key changes include: Addresses an issue that causes searchindexer.exe to stop responding during a dismount operation in the Remote Desktop setup environment. Addresses an issue that redirects the PowerShell command output so that transcript logs do not contain any content. Transcript logs might contain decrypted passwords if you turn PowerShell logging on. Consequently, the transcript logs lose the decrypted passwords. Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the internet after a client device connects. Addresses an issue that prevents the use of Encrypted File System (EFS) files over a Web-based Distributed Authoring and Versioning (WebDAV) connection. Addresses an issue that causes Microsoft NTLM authentication using an external trust to fail. This issue occurs when a domain controller that contains the January 11, 2022 or later Windows update services the authentication request, is not in a root domain, and does not hold the Global Catalog role. The affected operations might log the following errors: The security database has not been started. The domain was in the wrong state	KB5015808	Applicable on MS4000 Console

	to perform the security operation. 0xc00000dd (STATUS_INVALID_DOMAIN_STATE). Addresses an issue that causes the primary domain controller (PDC) of the root domain to generate warning and error events in the System log. This issue occurs when the PDC incorrectly tries to scan outgoing-only trusts. Addresses an issue that might damage BitLocker virtual machine-based (VM) system files if you expand the BitLocker partition while the VM is offline. Addresses a known issue that prevents Windows servers that use the Routing and Remote Access Service (RRAS) from correctly directing internet traffic. Devices that connect to the server might not connect to the internet, and servers might lose connection to the internet after a client device connects to them.		
2022-07 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.	KB5016058	Applicable on MS4000 Console
2022-07 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	This security update includes quality improvements. Key changes include: Addresses an issue that causes searchindexer.exe to stop responding during a dismount operation in the Remote Desktop setup environment. Addresses an issue that redirects the PowerShell command output so that transcript logs do not contain any content. Transcript logs might contain decrypted passwords if you turn PowerShell logging on. Consequently, the transcript logs lose the decrypted passwords. Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the internet after a client device connects. Addresses an issue that prevents the use of Encrypted File System (EFS) files over a Web-based Distributed Authoring and Versioning (WebDAV) connection. Addresses an issue that causes Microsoft NTLM authentication using an external trust to fail. This issue occurs when a domain controller that contains the January 11, 2022 or later Windows update services the authentication request, is not in a root domain, and does not hold the Global Catalog role. The affected operations might log the following errors: The security database has not been started. The domain was in the wrong state to perform the security operation. 0xc00000dd (STATUS_INVALID_DOMAIN_STATE). Addresses an issue that causes the primary domain controller (PDC) of the root domain to generate warning and error events in the System log. This issue occurs when the PDC incorrectly tries to scan outgoing-only trusts. Addresses an issue that might damage BitLocker virtual machine-based (VM) system files if you expand the BitLocker partition while	KB5015808	Applicable on MS4000 and Anesthesia System

	the VM is offline. Addresses a known issue that prevents Windows servers that use the Routing and Remote Access Service (RRAS) from correctly directing internet traffic. Devices that connect to the server might not connect to the internet, and servers might lose connection to the internet after a client device connects to them.		
2022-07 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.	KB5016058	Applicable on MS4000 and Anesthesia System
Windows Malicious Software Removal Tool - v5.103	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS4000 Console and MED3500 Console
2022-07 Security Only Quality Update for Windows Server 2008 for x86-based Systems	This security-only update includes new improvements for the following issues: When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects. Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic. Devices which connect to the server might not connect to the Internet, and servers can lose connection to the Internet after a client device connects.	KB5015870	Applicable on MS4000 Console and MED3500 Console
2022-07 Security Monthly Quality Rollup for Windows Server 2008 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5014752 (released June 14, 2022) and includes new improvements for the following issues: When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. NTLM authentication through an external trust is unsuccessful when serviced by a domain controller that has the January 11, 2022 or later Windows update installed. This issue occurs if the DC is in a non-root domain and does not hold the global catalog (GC) role. Impacted operations may log the following errors: The security database has not been started. The domain was in the wrong state to perform the security operation. 0xc00000dd (STATUS_INVALID_DOMAIN_STATE) Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host	KB5015866	Applicable on MS4000 Console and MED3500 Console

	device might lose the connection to the Internet after a client device connects. Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic. Devices which connect to the server might not connect to the Internet, and servers can lose connection to the Internet after a client device connects.		
2022-07 Servicing Stack Update for Windows Server 2008 for x86-based Systems	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) make sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.	KB5016129	Applicable on MS4000 Console and MED3500 Console
2022-07 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5014748 (released June 14, 2022) and includes new improvements for the following issues: When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. NTLM authentication through an external trust is unsuccessful when serviced by a domain controller that has the January 11, 2022 or later Windows update installed. This issue occurs if the DC is in a non-root domain and does not hold the global catalog (GC) role. Impacted operations may log the following errors: The security database has not been started. The domain was in the wrong state to perform the security operation. 0xc00000dd (STATUS_INVALID_DOMAIN_STATE) Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects. Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic. Devices which connect to the server might not connect to the Internet, and servers can lose connection to the Internet after a client device connects.	KB5015861	Applicable on MS4000 and Anesthesia System

2022-07 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This security-only update includes new improvements for the following issues: When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects. Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic. Devices which connect to the server might not connect to the Internet, and servers can lose connection to the Internet after a client device connects.	KB5015862	Applicable on MS4000 and Anesthesia System
2022-07 Servicing Stack Update for Windows Embedded Standard 7 for x86-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.	KB5016057	Applicable on MS4000 and Anesthesia System
2022-07 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems	This security update resolves vulnerabilities in Internet Explorer.	KB5015805	Applicable on MS4000 and Anesthesia System

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

bd.com

BD and the BD Logo are trademarks of Becton, Dickinson and Company or its affiliates. © 2022 BD. All rights reserved.

Security Patches: Security Module

July 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for July 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 - v5.102 (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.
2022-07 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems (KB5015805)	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.	KB5015805	Applicable on Security Module devices.
2022-07 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5015874)	This cumulative security update includes improvements that are part of update KB5014738 (released June 14, 2022) and includes new improvements for the following issues: • Starting with this release, we are displaying a dialog box to remind users about the End of Support (EOS) for Windows 8.1 in January 2023. If you click Remind me later, the dialog box will appear once every 35 days. If you click Remind me after the end of support date, the dialog box will not appear again until after the EOS date. This reminder does not appear on the following: • Managed Pro and Enterprise devices.	KB5015874	Applicable on Security Module devices.

	• Windows Embedded 8.1 Industry Enterprise and Windows Embedded 8.1 Industry Pro devices. • When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. • NTLM authentication through an external trust is unsuccessful when serviced by a domain controller that has the January 11, 2022 or later Windows update installed. This issue occurs if the DC is in a non-root domain and does not hold the global catalog (GC) role. Impacted operations may log the following errors:		
2022-07 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5015877)	This security-only update includes new improvements for the following issues: ▪ Starting with this release, we are displaying a dialog box to remind users about the End of Support (EOS) for Windows 8.1 in January 2023. If you click Remind me later, the dialog box will appear once every 35 days. If you click Remind me after the end of support date, the dialog box will not appear again until after the EOS date. This reminder does not appear on the following: ▪ Windows Embedded 8.1 Industry Enterprise and Windows Embedded 8.1 Industry Pro devices. ▪ When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. ▪ Applications might not run after an AppLocker publisher rule is deployed. ▪ Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects. ▪ Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic. Devices which connect to the server might not connect to the Internet, and servers can lose connection to the Internet after a client device connects.	KB5015877	Applicable on Security Module devices.
2022-07 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB5016264)	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.	KB5016264	Applicable on Security Module devices.
2022-07 Security and Quality Rollup for .NET Framework 3.5 for Windows Server 2012 R2 for x64 (KB5016268)	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.	KB5016268	Applicable on Security Module devices.

2022-07 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 (KB5016568)	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.	KB5016568	Applicable on Security Module devices.
2022-07 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5015808)	This security update includes quality improvements. Key changes include: ▪ Addresses an issue that causes searchindexer.exe to stop responding during a dismount operation in the Remote Desktop setup environment. ▪ Addresses an issue that redirects the PowerShell command output so that transcript logs do not contain any content. Transcript logs might contain decrypted passwords if you turn PowerShell logging on. Consequently, the transcript logs lose the decrypted passwords. ▪ Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the internet after a client device connects. ▪ Addresses an issue that prevents the use of Encrypted File System (EFS) files over a Web-based Distributed Authoring and Versioning (WebDAV) connection. ▪ Addresses an issue that causes Microsoft NTLM authentication using an external trust to fail. This issue occurs when a domain controller that contains the January 11, 2022 or later Windows update services the authentication request, is not in a root domain, and does not hold the Global Catalog role. The affected operations might log the following errors: ▪ Addresses an issue that causes the primary domain controller (PDC) of the root domain to generate warning and error events in the System log. This issue occurs when the PDC incorrectly tries to scan outgoing-only trusts. ▪ Addresses an issue that might damage BitLocker virtual machine-based (VM) system files if you expand the BitLocker partition while the VM is offline.	KB5015808	Applicable on Security Module devices.
2022-07 Servicing Stack Update for Windows Server 2016 for x64-based Systems (KB5016058)	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.	KB5016058	Applicable on Security Module devices.

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

bd.com

BD and the BD Logo are trademarks of Becton, Dickinson and Company or its affiliates. © 2022 BD. All rights reserved.

Security Patches: BD Pyxis™ IV Prep

July 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for July 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
2022-07 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5015877	Applicable on Cato

2022-07 Security and Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 for x64	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5016568	Applicable on Cato
2022-07 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5015805	Applicable on Cato
2022-07 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.	KB5015874	Applicable on Cato
2022-07 Servicing Stack Update for Windows Server 2012 R2 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.	KB5016264	Applicable on Cato
2022-07 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.	KB5015808	Applicable on Cato
2022-07 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.	KB5016058	Applicable on Cato

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

bd.com

BD and the BD Logo are trademarks of Becton, Dickinson and Company
or its affiliates. © 2022 BD. All rights reserved.

Security Patches: BD Pyxis Connect

July 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for July 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
2022-07 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5015808)	This security update includes quality improvements. Key changes include: • Addresses an issue that causes searchindexer.exe to stop responding during a dismount operation in the Remote Desktop setup environment. • Addresses an issue that redirects the PowerShell command output so that transcript logs do not contain any content. Transcript logs might contain decrypted passwords if you turn PowerShell logging on. Consequently, the transcript logs lose the decrypted passwords. • Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the internet after a client device connects. • Addresses an issue that prevents the use of Encrypted File System (EFS) files over a Web-based Distributed Authoring and Versioning (WebDAV) connection. • Addresses an issue that causes Microsoft NTLM authentication using an external trust to fail.	KB5015808	Applicable to Connect device.

2022-07 Servicing Stack Update for Windows Server 2016 for x64-based Systems (KB5016058)	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.	KB5016058	Applicable to Connect device.
Windows Malicious Software Removal Tool - v5.103 (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	Applicable to Connect device.
2022-07 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 (KB5016568)	This security update addresses an issue where the .NET Framework releases June 14, 2022-Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 (KB5013638) and Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 (KB5012139) were not cumulative and did not contain some previously released security updates. This security update includes all previous released security updates. There are no new security improvements being released in this update. - Improved the reliability of data-bound ComboBox controls under assistive technology.	KB5016568	Applicable to Connect device.

2022-07 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5015874)	This cumulative security update includes improvements that are part of update KB5014738 (released June 14, 2022) and includes new improvements for the following issues: • Starting with this release, we are displaying a dialog box to remind users about the End of Support (EOS) for Windows 8.1 in January 2023. If you click Remind me later, the dialog box will appear once every 35 days. If you click Remind me after the end of support date, the dialog box will not appear again until after the EOS date. This reminder does not appear on the following: - Managed Pro and Enterprise devices. - Windows Embedded 8.1 Industry Enterprise and Windows Embedded 8.1 Industry Pro devices. • When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. • NTLM authentication through an external trust is unsuccessful when serviced by a domain controller that has the January 11, 2022 or later Windows update installed. This issue occurs if the DC is in a non-root domain and does not hold the global catalog (GC) role. Impacted operations may log the following errors: - The security database has not been started. - The domain was in the wrong state to perform the security operation. - 0xc00000dd STATUS_INVALID_DOMAIN_STATE) • Applications might not run after an AppLocker publisher rule is deployed. • Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects. • Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic. Devices which connect to the server might not connect to the Internet, and servers can lose connection to the Internet after a client device connects.	KB5015874	Applicable to Connect device.

2022-07 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5015877)	This security-only update includes new improvements for the following issues: • Starting with this release, we are displaying a dialog box to remind users about the End of Support (EOS) for Windows 8.1 in January 2023. If you click Remind me later, the dialog box will appear once every 35 days. If you click Remind me after the end of support date, the dialog box will not appear again until after the EOS date. This reminder does not appear on the following: - Managed Pro and Enterprise devices. - Windows Embedded 8.1 Industry Enterprise and Windows Embedded 8.1 Industry Pro devices. • When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. • Applications might not run after an AppLocker publisher rule is deployed. • Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects. • Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic. Devices which connect to the server might not connect to the Internet, and servers can lose connection to the Internet after a client device connects.	KB5015877	Applicable to Connect device.
2022-07 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems (KB5015805)	This security update resolves vulnerabilities in Internet Explorer. This update applies to the following: - Internet Explorer 11 on Windows Server 2012 R2 - Internet Explorer 11 on Windows 8.1 - Internet Explorer 11 on Windows Server 2012 - Internet Explorer 11 on Windows Server 2008 R2 SP1 - Internet Explorer 11 on Windows 7 SP1	KB5015805	Applicable to Connect device.

2022-07 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB5016264)	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates. This update applies to the following: - Windows 8.1 for x86-based devices - Windows 8.1 for x64-based devices - Windows RT 8.1 - Windows Server 2012 R2 - Windows Server 2012 R2 (Server Core installation)	KB5016264	Applicable to Connect device.
2022-07 Dynamic Cumulative Update for Windows 10 Version 21H1 for x86-based Systems (KB5015807)	This security update Addresses security issues for your Windows operating system.	KB5015807	Applicable to Connect device.

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

bd.com

BD and the BD Logo are trademarks of Becton, Dickinson and Company or its affiliates. © 2022 BD. All rights reserved.

Security Patches: BD Pharmogistics

July 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for July 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.
2022-07 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB5016264) Last Modified: 7/12/2022	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.	KB5016264	Applicable on PLX, CII Safe and Infusion.

2022-07 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5015874) Last Modified: 7/12/2022	This cumulative security update includes improvements that are part of update KB5014738 (released June 14, 2022) and includes new improvements for the following issues: Starting with this release, we are displaying a dialog box to remind users about the End of Support (EOS) for Windows 8.1 in January 2023. Applications might not run after an AppLocker publisher rule is deployed. Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects.	KB5015874	Applicable on PLX, CII Safe and Infusion.
2022-07 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems (KB5015805) Last Modified: 7/12/2022	This security update resolves vulnerabilities in Internet Explorer. To learn more about these vulnerabilities, see Deployments - Security Update Guide.	KB5015805	Applicable on PLX, CII Safe and Infusion.
2022-07 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 (KB5016568) Last Modified: 7/12/2022	This security update addresses an issue where the .NET Framework releases June 14, 2022-Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 (KB5013638) and Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 (KB5012139) were not cumulative and did not contain some previously released security updates. This security update includes all previous released security updates. There are no new security improvements being released in this update.	KB5016568	Applicable on PLX, CII Safe and Infusion.

2022-07 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5015877) Last Modified: 7/12/2022	This security-only update includes new improvements for the following issues: Starting with this release, we are displaying a dialog box to remind users about the End of Support (EOS) for Windows 8.1 in January 2023. When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. Applications might not run after an AppLocker publisher rule is deployed. Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects. Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic. Devices which connect to the server might not connect to the Internet, and servers can lose connection to the Internet after a client device connects.	KB5015877	Applicable on PLX, CII Safe and Infusion.
2022-07 Servicing Stack Update for Windows Server 2016 for x64-based Systems (KB5016058) Last Modified: 7/12/2022	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.	KB5016058	Applicable on PLX, CII Safe and Infusion.

Security Update for Windows 10 Version 1909 for x64-based Systems (KB4535680)	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 on PLX, CII Safe and Infusion.
2022-07 Cumulative Update for Windows 10 Version 21H1 for x64-based Systems (KB5015807) Last Modified: 7/12/2022	Windows 10 servicing stack update - 19042.1790, 19043.1790, and 19044.1790 This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) ensure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.	KB5015807	Applicable on PLX, CII Safe and Infusion.

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

bd.com

BD and the BD Logo are trademarks of Becton, Dickinson and Company or its affiliates. © 2022 BD. All rights reserved.

Security Patches: TIM

July 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for July 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 - v5.103 (KB890830)	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.	KB890830	Applicable on TIM

2022-07 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 (KB5016568)	This security update addresses an issue where the .NET Framework releases June 14, 2022-Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 (KB5013638) and Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 (KB5012139) were not cumulative and did not contain some previously released security updates. This security update includes all previous released security updates. There are no new security improvements being released in this update.	KB5016568	Applicable on TIM
2022-07 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5015874)	This cumulative security update includes improvements that are part of update KB5014738 (released June 14, 2022) and includes new improvements for the following issues: Starting with this release, we are displaying a dialog box to remind users about the End of Support (EOS) for Windows 8.1 in January 2023. If you click Remind me later, the dialog box will appear once every 35 days. If you click Remind me after the end of support date, the dialog box will not appear again until after the EOS date. This reminder does not appear on the following: Managed Pro and Enterprise devices. Windows Embedded 8.1 Industry Enterprise and Windows Embedded 8.1 Industry Pro devices. When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. NTLM authentication through an external trust is unsuccessful when serviced by a domain controller that has the January 11, 2022 or later Windows update installed. This issue occurs if the DC is in a non-root domain and does not hold the global catalog (GC) role. Impacted operations may log the following errors: The security database has not been started.	KB5015874	Applicable on TIM

	The domain was in the wrong state to perform the security operation. 0xc00000dd (STATUS_INVALID_DOMAIN_STATE) Applications might not run after an AppLocker publisher rule is deployed. Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects. Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic. Devices which connect to the server might not connect to the Internet, and servers can lose connection to the Internet after a client device connects.		
2022-07 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB5016264)	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates. This update applies to the following: Windows 8.1 for x86-based devices Windows 8.1 for x64-based devices Windows RT 8.1 Windows Server 2012 R2 Windows Server 2012 R2 (Server Core installation) This security update includes quality improvements. Key changes include:	KB5016264	Applicable on TIM

2022-07 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5015808)	Addresses an issue that causes searchindexer.exe to stop responding during a dismount operation in the Remote Desktop setup environment. Addresses an issue that redirects the PowerShell command output so that transcript logs do not contain any content. Transcript logs might contain decrypted passwords if you turn PowerShell logging on. Consequently, the transcript logs lose the decrypted passwords. Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the internet after a client device connects. Addresses an issue that prevents the use of Encrypted File System (EFS) files over a Web-based Distributed Authoring and Versioning (WebDAV) connection. Addresses an issue that causes Microsoft NTLM authentication using an external trust to fail. This issue occurs when a domain controller that contains the January 11, 2022 or later Windows update services the authentication request, is not in a root domain, and does not hold the Global Catalog role. The affected operations might log the following errors: The security database has not been started. The domain was in the wrong state to perform the security operation. 0xc00000dd (STATUS_INVALID_DOMAIN_STATE). Addresses an issue that causes the primary domain controller (PDC) of the root domain to generate warning and error events in the System log. This issue occurs when the PDC incorrectly tries to scan outgoing-only trusts. Addresses an issue that might damage BitLocker virtual machine-based (VM) system files if you expand the BitLocker partition while the VM is offline. Addresses a known issue that prevents Windows servers that use the Routing and Remote Access Service (RRAS) from correctly directing internet traffic. Devices that connect to the server might not connect to the internet, and servers might lose	KB5015808	Applicable on TIM

connection to the internet after a client device connects to them.

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 July 2022 Security Updates.

2022-07 Servicing Stack Update for Windows Server 2016 for x64-based Systems (KB5016058)	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. IMPORTANT Windows 10, version 1607 reached end of service on April 9, 2019 for devices running the Enterprise, Education, and IoT Enterprise editions. After April 9, 2019, these devices will no longer be offered servicing stack updates. To continue receiving these updates, we recommend updating to the latest version of Windows. For information about the end of service for Windows 10, version 1607, see here. For information about the end of service for Windows Server 2016, see here. This update applies to: Windows 10, version 1607 for x86-based devices Windows 10, version 1607 for x64-based devices Windows Server 2016 Windows Server 2016 (Server Core installation)	KB5016058	Applicable on TIM

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

bd.com

BD and the BD Logo are trademarks of Becton, Dickinson and Company or its affiliates. © 2022 BD. All rights reserved.

Security Patches: BD FHIR

July 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for July 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
2022-07 Cumulative update for windows server 2019 for x64 based systems (KB5015811)	This update addresses security issues for your Windows operating system. This security update includes improvements that were a part of update KB5014669 (released June 23, 2022) and also addresses the following issues: Addresses an issue that redirects the PowerShell command output so that transcript logs do not contain any content. Transcript logs might contain decrypted passwords if you turn PowerShell logging on. Consequently, the transcript logs lose the decrypted passwords.	**KB5015811**
2021-01 Update for windows server 2019 for x64 based systems (KB4589208)	This new release includes a microcode update from Intel for some CPUs. This update is a standalone update that is targeted at Windows 10, version 1809 and Windows Server 2019. This update also includes Intel microcode updates that were already released for these operating systems at the time of release.	**KB4589208**

Security update for Windows server 2019 for x64 based systems (KB4535680)	This security update makes improvements to Secure Boot DBX for the supported Windows versions. 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. This security update addresses the vulnerability by adding the signatures of the known vulnerable UEFI modules to the DBX.	**KB4535680**

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

bd.com

BD and the BD Logo are trademarks of Becton, Dickinson and Company or its affiliates. © 2022 BD. All rights reserved.

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

July 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for July 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 - v5.103	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 Anesthesia device.
2022-07 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.	KB5015811	Applicable on Anesthesia device.

2022-07 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.	KB5016058	Applicable on Anesthesia device.
2022-07 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	This security update includes quality improvements. Key changes include: Addresses an issue that causes searchindexer.exe to stop responding during a dismount operation in the Remote Desktop setup environment. Addresses an issue that redirects the PowerShell command output so that transcript logs do not contain any content. Transcript logs might contain decrypted passwords if you turn PowerShell logging on. Consequently, the transcript logs lose the decrypted passwords. Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the internet after a client device connects. Addresses an issue that prevents the use of Encrypted File System (EFS) files over a Web-based Distributed Authoring and Versioning (WebDAV) connection. Addresses an issue that causes Microsoft NTLM authentication using an external trust to fail. This issue occurs when a domain controller that contains the January 11, 2022 or later Windows update services the authentication request, is not in a root domain, and does not hold the Global Catalog role. The affected operations might log the following errors: The security database has not been started. The domain was in the wrong state to perform the security operation. 0xc00000dd (STATUS_INVALID_DOMAIN_STATE). Addresses an issue that causes the primary domain controller (PDC) of the root domain to generate warning and error events in the System log. This issue occurs when the PDC incorrectly tries to scan outgoing-only trusts. Addresses an issue that might damage BitLocker virtual machine-based (VM) system files if you expand the BitLocker partition while the VM is offline. Addresses a known issue that prevents Windows servers that use the Routing and Remote Access Service (RRAS) from correctly directing internet traffic. Devices that connect to the server might not connect to the internet, and servers might lose connection to the internet after a client device connects to them.	KB5015808	Applicable on Anesthesia device.
2022-07 Servicing Stack Update for Windows Embedded Standard 7 for x86-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.	KB5016057	Applicable on Anesthesia device.

2022-07 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5014748 (released June 14, 2022) and includes new improvements for the following issues: When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. NTLM authentication through an external trust is unsuccessful when serviced by a domain controller that has the January 11, 2022 or later Windows update installed. This issue occurs if the DC is in a non-root domain and does not hold the global catalog (GC) role. Impacted operations may log the following errors: The security database has not been started. The domain was in the wrong state to perform the security operation. 0xc00000dd (STATUS_INVALID_DOMAIN_STATE) Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects.	KB5015861	Applicable on Anesthesia device.
2022-07 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This security-only update includes new improvements for the following issues: When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects. Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic.	KB5015862	Applicable on Anesthesia device.

2022-07 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems	This security update resolves vulnerabilities in Internet Explorer.	KB5015805	Applicable on Anesthesia device.

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

bd.com

BD and the BD Logo are trademarks of Becton, Dickinson and Company or its affiliates. © 2022 BD. All rights reserved.

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

July 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for July 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 - v5.103	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	Applicable on CIIsafe, MedSTN, Anesthesia device.
2022-07 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.	KB5015811	Applicable on CIIsafe, MedSTN, Anesthesia device.

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

bd.com

BD and the BD Logo are trademarks of Becton, Dickinson and Company or its affiliates. © 2022 BD. All rights reserved.

Security Patches: BD Pyxis™ Supply

July 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for July 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
2022-07 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5015877)	This security-only update includes new improvements for the following issues: • Starting with this release, we are displaying a dialog box to remind users about the End of Support (EOS) for Windows 8.1 in January 2023. If you click Remind me later, the dialog box will appear once every 35 days. If you click Remind me after the end of support date, the dialog box will not appear again until after the EOS date. This reminder does not appear on the following: • Managed Pro and Enterprise devices. • Windows Embedded 8.1 Industry Enterprise and Windows Embedded 8.1 Industry Pro devices. • When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. • Applications might not run after an AppLocker publisher rule is deployed. • Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects.	KB5015877	Applicable on Supply.

	• Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic. Devices which connect to the server might not connect to the Internet, and servers can lose connection to the Internet after a client device connects.		
2022-07 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 (KB5016568)2022-07 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 (KB5016568)	This security update addresses an issue where the .NET Framework releases June 14, 2022-Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 (KB5013638) and Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 (KB5012139) were not cumulative and did not contain some previously released security updates. This security update includes all previous released security updates. There are no new security improvements being released in this update.	KB5016568	Applicable on Supply.
2022-07 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems (KB5015805)	This security update resolves vulnerabilities in Internet Explorer. To learn more about these vulnerabilities, see Deployments - Security Update Guide.This security update resolves vulnerabilities in Internet Explorer. To learn more about these vulnerabilities, see Deployments - Security Update Guide.	KB5015805	Applicable on Supply.
2022-07 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems (KB5015805)	This security update resolves vulnerabilities in Internet Explorer. To learn more about these vulnerabilities, see Deployments - Security Update Guide.This security update resolves vulnerabilities in Internet Explorer. To learn more about these vulnerabilities, see Deployments - Security Update Guide.	KB5015805	Applicable on Supply.
2022-07 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5015874)	This cumulative security update includes improvements that are part of update KB5014738 (released June 14, 2022) and includes new improvements for the following issues: • Starting with this release, we are displaying a dialog box to remind users about the End of Support (EOS) for Windows 8.1 in January 2023. If you click Remind me later, the dialog box will appear once every 35 days. If you	KB5015874	Applicable on Supply.

	click Remind me after the end of support date, the dialog box will not appear again until after the EOS date. This reminder does not appear on the following: • Managed Pro and Enterprise devices. • Windows Embedded 8.1 Industry Enterprise and Windows Embedded 8.1 Industry Pro devices. • When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. • NTLM authentication through an external trust is unsuccessful when serviced by a domain controller that has the January 11, 2022 or later Windows update installed. This issue occurs if the DC is in a non-root domain and does not hold the global catalog (GC) role. Impacted operations may log the following errors: • The security database has not been started. • The domain was in the wrong state to perform the security operation. • 0xc00000dd (STATUS_INVALID_DOMAIN_STATE) • Applications might not run after an AppLocker publisher rule is deployed. • Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects. • Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic. Devices which connect to the server might not connect to the Internet, and servers can lose connection to the Internet after a client device connects.		
2022-07 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB5016264)	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.	KB5016264	Applicable on Supply.

2022-07 Servicing Stack Update for Windows Embedded Standard 7 for x86-based Systems (KB5016057)	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.	KB5016057	Applicable on Supply.
2022-07 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems (KB5015862)	This security-only update includes new improvements for the following issues: • When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. • Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects. • Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic. Devices which connect to the server might not connect to the Internet, and servers can lose connection to the Internet after a client device connects.	KB5015862	Applicable on Supply.
2022-07 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems (KB5015861)	This cumulative security update contains improvements that are part of update KB5014748 (released June 14, 2022) and includes new improvements for the following issues: • When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. • NTLM authentication through an external trust is unsuccessful when serviced by a domain controller that has the January 11, 2022 or later Windows update installed. This issue occurs if the DC is in a non-root domain and does not hold the global catalog (GC) role. Impacted operations may log the following errors: • The security database has not been started. • The domain was in the wrong state to perform the security operation. • 0xc00000dd (STATUS_INVALID_DOMAIN_STATE) • Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature,	KB5015861	Applicable on Supply.

	the host device might lose the connection to the Internet after a client device connects. • Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic. Devices which connect to the server might not connect to the Internet, and servers can lose connection to the Internet after a client device connects.		
2022-07 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5015808)	This security update includes quality improvements. Key changes include: • Addresses an issue that causes searchindexer.exe to stop responding during a dismount operation in the Remote Desktop setup environment. • Addresses an issue that redirects the PowerShell command output so that transcript logs do not contain any content. Transcript logs might contain decrypted passwords if you turn PowerShell logging on. Consequently, the transcript logs lose the decrypted passwords. • Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the internet after a client device connects. • Addresses an issue that prevents the use of Encrypted File System (EFS) files over a Web-based Distributed Authoring and Versioning (WebDAV) connection. • Addresses an issue that causes Microsoft NTLM authentication using an external trust to fail. This issue occurs when a domain controller that contains the January 11, 2022 or later Windows update services the authentication request, is not in a root domain, and does not hold the Global Catalog role. The affected operations might log the following errors: • The security database has not been started. • The domain was in the wrong state to perform the security operation. • 0xc00000dd (STATUS_INVALID_DOMAIN_STATE). • Addresses an issue that causes the primary domain controller (PDC) of the root domain to generate warning and error events in the System log. This issue occurs when the PDC incorrectly tries to scan outgoing-only trusts.	KB5015808	Applicable on Supply.

	• Addresses an issue that might damage BitLocker virtual machine-based (VM) system files if you expand the BitLocker partition while the VM is offline. • Addresses a known issue that prevents Windows servers that use the Routing and Remote Access Service (RRAS) from correctly directing internet traffic. Devices that connect to the server might not connect to the internet, and servers might lose connection to the internet after a client device connects to them.		
2022-07 Cumulative Update for Windows 10 Version 1607 for x64-based Systems (KB5015808)	This security update includes quality improvements. Key changes include: • Addresses an issue that causes searchindexer.exe to stop responding during a dismount operation in the Remote Desktop setup environment. • Addresses an issue that redirects the PowerShell command output so that transcript logs do not contain any content. Transcript logs might contain decrypted passwords if you turn PowerShell logging on. Consequently, the transcript logs lose the decrypted passwords. • Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the internet after a client device connects. • Addresses an issue that prevents the use of Encrypted File System (EFS) files over a Web-based Distributed Authoring and Versioning (WebDAV) connection. • Addresses an issue that causes Microsoft NTLM authentication using an external trust to fail. This issue occurs when a domain controller that contains the January 11, 2022 or later Windows update services the authentication request, is not in a root domain, and does not hold the Global Catalog role. The affected operations might log the following errors: • The security database has not been started. • The domain was in the wrong state to perform the security operation. • 0xc00000dd (STATUS_INVALID_DOMAIN_STATE). • Addresses an issue that causes the primary domain controller (PDC) of the root domain to generate warning and error events in the	KB5015808	Applicable on Supply.

	System log. This issue occurs when the PDC incorrectly tries to scan outgoing-only trusts. • Addresses an issue that might damage BitLocker virtual machine-based (VM) system files if you expand the BitLocker partition while the VM is offline. • Addresses a known issue that prevents Windows servers that use the Routing and Remote Access Service (RRAS) from correctly directing internet traffic. Devices that connect to the server might not connect to the internet, and servers might lose connection to the internet after a client device connects to them.		
2022-07 Servicing Stack Update for Windows Server 2016 for x64-based Systems (KB5016058)	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.	KB5016058	Applicable on Supply.
2022-07 Servicing Stack Update for Windows 10 Version 1607 for x64-based Systems (KB5016058)	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.	KB5016058	Applicable on Supply.
2022-07 Cumulative Update for Windows Server 2019 for x64-based Systems (KB5015811)	This security update includes improvements that were a part of update KB5014669 (released June 23, 2022) and also addresses the following issues: • Addresses an issue that redirects the PowerShell command output so that transcript logs do not contain any content. Transcript logs might contain decrypted passwords if you turn PowerShell logging on. Consequently, the transcript logs lose the decrypted passwords.	KB5015811	Applicable on Supply.

2022-07 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB5015811)	This security update includes improvements that were a part of update KB5014669 (released June 23, 2022) and also addresses the following issues: • Addresses an issue that redirects the PowerShell command output so that transcript logs do not contain any content. Transcript logs might contain decrypted passwords if you turn PowerShell logging on. Consequently, the transcript logs lose the decrypted passwords.	KB5015811	Applicable on Supply.
Windows Malicious Software Removal Tool x64 - v5.103	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.
2022-07 Servicing Stack Update for Windows Server 2008 for x86-based Systems (KB5016129)	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) make sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.	KB5016129	Applicable on Supply.
2022-07 Security Only Quality Update for Windows Server 2008 for x86-based Systems (KB5015870)	This security-only update includes new improvements for the following issues: • When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. • Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects. • Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic. Devices which connect to the server might not connect to the Internet, and servers can lose connection to the Internet after a client device connects.	KB5015870	Applicable on Supply.

2022-07 Security Monthly Quality Rollup for Windows Server 2008 for x86-based Systems (KB5015866)	This cumulative security update contains improvements that are part of update KB5014752 (released June 14, 2022) and includes new improvements for the following issues: • When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. • NTLM authentication through an external trust is unsuccessful when serviced by a domain controller that has the January 11, 2022 or later Windows update installed. This issue occurs if the DC is in a non-root domain and does not hold the global catalog (GC) role. Impacted operations may log the following errors: • The security database has not been started. • The domain was in the wrong state to perform the security operation. • 0xc00000dd (STATUS_INVALID_DOMAIN_STATE) • Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects. • Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic. Devices which connect to the server might not connect to the Internet, and servers can lose connection to the Internet after a client device connects.	KB5015866	Applicable on Supply.

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

bd.com

BD and the BD Logo are trademarks of Becton, Dickinson and Company or its affiliates. © 2022 BD. All rights reserved.

Security Patches:
BD Pyxis™ Med Station ES

July 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for July 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 - v5.103	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 Med station device.
2022-07 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.	KB5015811	Applicable on Med station device.

2022-07 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5015805	Applicable on Med station device.
2022-07 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.	KB5015874	Applicable on Med station device.
2022-07 Security and Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 for x64	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5016568	Applicable on Med station device.
2022-07 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5015877	Applicable on Med station device.
2022-07 Servicing Stack Update for Windows Server 2012 R2 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.	KB5016264	Applicable on Med station device.
2022-07 Servicing Stack Update for Windows Embedded Standard 7 for x86-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.	KB5016057	Applicable on Med station device.

2022-07 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5014748 (released June 14, 2022) and includes new improvements for the following issues: When you use Encrypting File System (EFS) files over a remote Web Distributed Authoring and Versioning (WebDAV) protocol connection, the connection might be unsuccessful. NTLM authentication through an external trust is unsuccessful when serviced by a domain controller that has the January 11, 2022 or later Windows update installed. This issue occurs if the DC is in a non-root domain and does not hold the global catalog (GC) role. Impacted operations may log the following errors: The security database has not been started. The domain was in the wrong state to perform the security operation. 0xc00000dd (STATUS_INVALID_DOMAIN_STATE) Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the Internet after a client device connects. Addresses a known issue in which Windows Servers that use the Routing and Remote Access Service (RRAS) might be unable to correctly direct Internet traffic. Devices which connect to the server might not connect to the Internet, and servers can lose connection to the Internet after a client device connects.	KB5015861	Applicable on Med station device.
2022-07 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems.	This security update resolves vulnerabilities in Internet Explorer.	KB5015805	Applicable on Med station device.
2022-07 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.	KB5016058	Applicable on Med station device.
2022-07 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	This security update includes quality improvements. Key changes include: Addresses an issue that causes searchindexer.exe to stop responding during a dismount operation in the Remote Desktop setup environment. Addresses an issue that redirects the PowerShell command output so that transcript logs do not contain any content. Transcript logs might contain decrypted passwords if you turn PowerShell logging on. Consequently, the transcript logs lose the decrypted passwords. Addresses a known	KB5015808	Applicable on Med station device.

	issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the internet after a client device connects. Addresses an issue that prevents the use of Encrypted File System (EFS) files over a Web-based Distributed Authoring and Versioning (WebDAV) connection. Addresses an issue that causes Microsoft NTLM authentication using an external trust to fail. This issue occurs when a domain controller that contains the January 11, 2022 or later Windows update services the authentication request, is not in a root domain, and does not hold the Global Catalog role. The affected operations might log the following errors: The security database has not been started. The domain was in the wrong state to perform the security operation. 0xc00000dd (STATUS_INVALID_DOMAIN_STATE). Addresses an issue that causes the primary domain controller (PDC) of the root domain to generate warning and error events in the System log. This issue occurs when the PDC incorrectly tries to scan outgoing-only trusts. Addresses an issue that might damage BitLocker virtual machine-based (VM) system files if you expand the BitLocker partition while the VM is offline. Addresses a known issue that prevents Windows servers that use the Routing and Remote Access Service (RRAS) from correctly directing internet traffic. Devices that connect to the server might not connect to the internet, and servers might lose connection to the internet after a client device connects to them.		
2022-07 Cumulative Update for Windows Server 2016 for x64-based Systems	This security update includes quality improvements. Key changes include: Addresses an issue that causes searchindexer.exe to stop responding during a dismount operation in the Remote Desktop setup environment. Addresses an issue that redirects the PowerShell command output so that transcript logs do not contain any content. Transcript logs might contain decrypted passwords if you turn PowerShell logging on. Consequently, the transcript logs lose the decrypted passwords. Addresses a known issue that might prevent you from using the Wi-Fi hotspot feature. When attempting to use the hotspot feature, the host device might lose the connection to the internet after a client device connects. Addresses an issue that prevents the use of Encrypted File System (EFS) files over a Web-based Distributed Authoring and Versioning (WebDAV) connection. Addresses an issue that causes Microsoft NTLM authentication using an external trust to fail. This issue occurs when a domain controller that contains the January 11, 2022 or later Windows update services the authentication request, is not in a root domain, and does not hold the Global Catalog role. The affected operations might log the following errors: The security database has not been started. The domain was in the wrong state to perform the security operation. 0xc00000dd	KB5015808	Applicable on Med station device.

	(STATUS_INVALID_DOMAIN_STATE). Addresses an issue that causes the primary domain controller (PDC) of the root domain to generate warning and error events in the System log. This issue occurs when the PDC incorrectly tries to scan outgoing-only trusts. Addresses an issue that might damage BitLocker virtual machine-based (VM) system files if you expand the BitLocker partition while the VM is offline. Addresses a known issue that prevents Windows servers that use the Routing and Remote Access Service (RRAS) from correctly directing internet traffic. Devices that connect to the server might not connect to the internet, and servers might lose connection to the internet after a client device connects to them.		
2022-07 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.	KB5016058	Applicable on Med station device.
2022-07 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.	KB5015811	Applicable on Server.
2022-05 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10 Version for x64	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5013868	Applicable on Server.

2022-05 Cumulative Update preview for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10 Version 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.	KB5014090	Applicable on Server.

2022-05 Cumulative Update Preview for Windows Server 2019 (1809) 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.	KB5014022	Applicable on Server.

2022-05 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 10 Version for x64	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5013868	Applicable on Server.

2022-05 Cumulative Update for Windows Server 2019 (1809) for x64-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5013941	Applicable on Server.

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

bd.com

BD and the BD Logo are trademarks of Becton, Dickinson and Company or its affiliates. © 2022 BD. All rights reserved.