BD Product Name: **BD Pyxis™ Security Module**

Date of Critical or Security Patches: July 2021
Abstract: Critical or Security Patches – July 2021

Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for July 2021. These patches were not found to adversely affect BD products and will be applied according to customers' service agreement.

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).

Patch Name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.90	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 7 Windows Server 2008 R2 for x64-based Systems	KB890830	N/A
2021-07 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems	This security update includes improvements and fixes that were a part of update KB5004954 (released July 6, 2021) and addresses the following issues: • Addresses an issue in which 16-bit applications fail with an error message that states a general fault in VBRUN300.DLL • Addresses an issue in which some EMFs built by using third-party applications that	KB5004298	N/A

	use ExtCreatePen and ExtCreateFontIndirect render incorrectly • Adds Advanced Encryption Standard (AES) encryption protections • Removes support for the PerformTicketSignature setting and permanently enables Enforcement mode		
2021-07 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems	This security update includes improvements and fixes that were a part of update KB5003671 (released June 8, 2021)	KB5004954	N/A
2021-07 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems	This security update includes quality improvements. Key changes include: • Addresses a remote code execution exploit in the Windows Print Spooler service, known as “PrintNightmare”. After installing this and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system’s Trusted Root Certification Authorities trusts signed drivers.	KB5004958	N/A

BD Product Name: **BD Pyxis™ Pharmogistics™**
Date of Critical or Security Patches: July 2021
Abstract: Critical or Security Patches – July 2021

Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for July 2021. These patches were not found to adversely affect BD products and will be applied according to customers' service agreement.

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).

Patch Name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.85	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 7 Windows Server 2008 R2 for x64-based Systems	KB890830	N/A
2020-07 Extended Security Updates (ESU) Licensing Preparation Package for Windows Server 2008 R2 for x64-based Systems (KB4575903)	**Description:** This update provides the complete set of licensing changes to enable installation of the ESU MAK add-on key, which is one of the steps to prepare for installation of Extended Security Updates. (For the full set of steps, please see KB4522133). A reboot is required after installing this update.	KB4575903	N/A
2021-07 Security Monthly Quality Rollup for Windows Server 2012	This security update includes improvements and fixes that were a part of update KB5003671 (released	KB5004954	N/A

R2 for x64-based Systems (KB5004954)	June 8, 2021) and addresses the following issues: • Addresses a remote code execution exploit in the Windows Print Spooler service, known as “PrintNightmare”, as documented in CVE-2021-34527.		
2021-07 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5004958)	This security update includes quality improvements. Key changes include: • Addresses a remote code execution exploit in the Windows Print Spooler service, known as “PrintNightmare”, as documented in CVE-2021-34527.	KB5004958	N/A
2020-12 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB4592495)	This security update includes quality improvements. Key changes include: • Security updates to Windows Graphics, Windows Peripherals, and Windows Core Networking.	KB4592495	N/A
2021-07 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5004948)	This security update includes quality improvements. Key changes include: • Addresses a remote code execution exploit in the Windows Print Spooler service, known as “PrintNightmare”, as	KB5004948	N/A

	documented in CVE-2021-34527.		
2021-07 Dynamic Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB5004945)	Updates a remote code execution exploit in the Windows Print Spooler service, known as “PrintNightmare”, as documented in CVE-2021-34527.	KB5004945	N/A
2021-07 Dynamic Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB5004237)	• Updates for verifying usernames and passwords. • Updates to improve security when Windows performs basic operations. • Updates an issue that might make printing to certain printers difficult. This issue affects various brands and models, but primarily receipt or label printers that connect using a USB port. After installing this update, you do not need to use a Known Issue Rollback (KIR) or a special Group Policy to resolve this issue.	KB5004237	N/A

BD Product Name: **BD Pyxis™ Anesthesia Station 4000**

Date of Critical or Security Patches: July 2021
Abstract: Critical or Security Patches – July 2021

Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for July 2021. These patches were not found to adversely affect BD products and will be applied according to customers' service agreement.

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).

Patch Name	Description	Patch ID	Notes
2021-07 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	This security update includes key changes as follows: Updates a remote code execution exploit in the Windows Print Spooler service, known as "PrintNightmare", as documented in CVE-2021-34527.	KB5004948	N/A
Windows Malicious Software Removal Tool x64 - v5.91	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	N/A
2021-07 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This security update includes improvements and fixes that were a part of update KB5003667 (released June 8, 2021) and addresses the following issues: Addresses a remote code execution exploit in the Windows Print Spooler service, known as "PrintNightmare", as documented in CVE-2021-34527. After installing this and later Windows updates,	KB5004953	N/A

	users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system's Trusted Root Certification Authorities trusts signed drivers. Microsoft recommends that you immediately install this update on all supported Windows client and server operating system, starting with devices that currently host the print server role. You also have the option to configure the RestrictDriverInstallationToAdministrators registry setting to prevent non-administrators from installing signed printer drivers on a print server. For more information, see KB5005010.		
2021-07 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	This security update includes quality improvements. Key changes include: Removes support for the PerformTicketSignature setting and permanently enables Enforcement mode for CVE-2020-17049. For more information and steps to enable full protection on domain controller servers, see Managing deployment of Kerberos S4U changes for CVE-2020-17049. Addresses an issue that incorrectly renders some Enhanced Metafile Format (EMF) files. This issue occurs if you build the EMF files using third-party applications	KB5004238	N/A

	with ExtCreatePen() and ExtCreateFontIndirect(). Addresses a redirector stop error that is caused by a race condition that occurs when the system deletes binding objects when connections close. Removes the Adobe Flash component from your device.		
2021-07 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This security update includes quality improvements. Key changes include: Addresses a remote code execution exploit in the Windows Print Spooler service, known as "PrintNightmare", as documented in CVE-2021-34527. After installing this and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system's Trusted Root Certification Authorities trusts signed drivers. Microsoft recommends that you immediately install this update on all supported Windows client and server operating system, starting with devices that currently host the print server role. You also have the option to configure the RestrictDriverInstallationToAdministrators registry setting to prevent non-administrators from installing signed printer drivers on a print server. For more information, see KB5005010.	KB5004951	N/A

BD Product Name: **BD Pyxis™ Anesthesia System 3500**

Date of Critical or Security Patches: July 2021
Abstract: Critical or Security Patches – July 2021

Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for July 2021. These patches were not found to adversely affect BD products and will be applied according to customers' service agreement.

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).

Patch Name	Description	Patch ID	Notes
2021-07 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This security update includes quality improvements. Key changes include: Addresses a remote code execution exploit in the Windows Print Spooler service, known as "PrintNightmare", as documented in CVE-2021-34527. After installing this and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system's Trusted Root Certification Authorities trusts signed drivers. Microsoft recommends that you immediately install this update on all supported Windows client and server operating system, starting with devices that currently host the print server role. You also have the option to configure the	KB5004951	N/A

	RestrictDriverInstallationToAdministrators registry setting to prevent non-administrators from installing signed printer drivers on a print server. For more information, see KB5005010.		
2021-07 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This security update includes improvements and fixes that were a part of update KB5003667 (released June 8, 2021) and addresses the following issues: Addresses a remote code execution exploit in the Windows Print Spooler service, known as “PrintNightmare”, as documented in CVE-2021-34527. After installing this and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system’s Trusted Root Certification Authorities trusts signed drivers. Microsoft recommends that you immediately install this update on all supported Windows client and server operating system, starting with devices that currently host the print server role. You also have the option to configure the RestrictDriverInstallationToAdministrators registry setting to prevent non-administrators from installing signed printer drivers on a print server. For more information, see KB5005010.	KB5004953	N/A

Windows Malicious Software Removal Tool - v5.91	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers	KB890830	N/A

BD Product Name: **BD Pyxis™ MedStation™ 3500**

Date of Critical or Security Patches: July 2021
Abstract: Critical or Security Patches – July 2021

Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for July 2021. These patches were not found to adversely affect BD products and will be applied according to customers' service agreement.

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).

Patch Name	Description	Patch ID	Notes
2021-07 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This security update includes quality improvements. Key changes include: Addresses a remote code execution exploit in the Windows Print Spooler service, known as "PrintNightmare", as documented in CVE-2021-34527. After installing this and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system's Trusted Root Certification Authorities trusts signed drivers. Microsoft recommends that you immediately install this update on all supported Windows client and server operating system, starting with devices that currently host the print server role. You also have the option to configure the	KB5004951	N/A

	RestrictDriverInstallationToAdministrators registry setting to prevent non-administrators from installing signed printer drivers on a print server. For more information, see KB5005010.		
2021-07 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This security update includes improvements and fixes that were a part of update KB5003667 (released June 8, 2021) and addresses the following issues: Addresses a remote code execution exploit in the Windows Print Spooler service, known as “PrintNightmare”, as documented in CVE-2021-34527. After installing this and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system’s Trusted Root Certification Authorities trusts signed drivers. Microsoft recommends that you immediately install this update on all supported Windows client and server operating system, starting with devices that currently host the print server role. You also have the option to configure the RestrictDriverInstallationToAdministrators registry setting to prevent non-administrators from installing signed printer drivers on a print server. For more information, see KB5005010.	KB5004953	N/A

2021-07 Security Monthly Quality Rollup for Windows Server 2008 for x86-based Systems	This security update includes improvements and fixes that were a part of update KB5003661 (released June 8, 2021) and addresses the following issues: Addresses a remote code execution exploit in the Windows Print Spooler service, known as “PrintNightmare”, as documented in CVE-2021-34527. After installing this and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system’s Trusted Root Certification Authorities trusts signed drivers. Microsoft recommends that you immediately install this update on all supported Windows client and server operating system, starting with devices that currently host the print server role. You also have the option to configure the RestrictDriverInstallationToAdministrators registry setting to prevent non-administrators from installing signed printer drivers on a print server. For more information, see KB5005010.	KB5004955	N/A
2021-07 Security Only Quality Update for Windows Server 2008 for x86-based Systems	This security update includes quality improvements. Key changes include: Addresses a remote code execution exploit in the Windows Print Spooler service, known as	KB5004959	N/A

	"PrintNightmare", as documented in CVE-2021-34527. After installing this and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system's Trusted Root Certification Authorities trusts signed drivers. Microsoft recommends that you immediately install this update on all supported Windows client and server operating system, starting with devices that currently host the print server role. You also have the option to configure the RestrictDriverInstallationToAdministrators registry setting to prevent non-administrators from installing signed printer drivers on a print server. For more information, see KB5005010.		

BD Product Name: **BD Pyxis™ MedStation™ 4000**

Date of Critical or Security Patches: July 2021
Abstract: Critical or Security Patches – July 2021

Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for July 2021. These patches were not found to adversely affect BD products and will be applied according to customers' service agreement.

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).

Patch Name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.91	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	N/A
2021-07 Cumulative Update for Windows Server 2016 for x64-based Systems	This security update includes key changes as follows: Updates a remote code execution exploit in the Windows Print Spooler service, known as "PrintNightmare", as documented in CVE-2021-34527.	KB5004948	N/A
2021-07 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	This security update includes quality improvements. Key changes include: Removes support for the PerformTicketSignature setting and permanently enables Enforcement mode for CVE-2020-17049. For more information and steps to enable full protection on domain controller servers, see Managing deployment of Kerberos S4U changes for CVE-2020-17049.	KB5004238	N/A

	Addresses an issue that incorrectly renders some Enhanced Metafile Format (EMF) files. This issue occurs if you build the EMF files using third-party applications with ExtCreatePen() and ExtCreateFontIndirect(). Addresses a redirector stop error that is caused by a race condition that occurs when the system deletes binding objects when connections close. Removes the Adobe Flash component from your device.		
2021-07 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	This security update includes key changes as follows: Updates a remote code execution exploit in the Windows Print Spooler service, known as "PrintNightmare", as documented in CVE-2021-34527.	KB5004948	N/A
2021-07 Security Monthly Quality Rollup for Windows Server 2008 for x86-based Systems	This security update includes improvements and fixes that were a part of update KB5003661 (released June 8, 2021) and addresses the following issues: Addresses a remote code execution exploit in the Windows Print Spooler service, known as "PrintNightmare", as documented in CVE-2021-34527. After installing this and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in	KB5004955	N/A

	the system's Trusted Root Certification Authorities trusts signed drivers. Microsoft recommends that you immediately install this update on all supported Windows client and server operating system, starting with devices that currently host the print server role. You also have the option to configure the RestrictDriverInstallationToAdministrators registry setting to prevent non-administrators from installing signed printer drivers on a print server. For more information, see KB5005010.		
2021-07 Security Only Quality Update for Windows Server 2008 for x86-based Systems	This security update includes quality improvements. Key changes include: Addresses a remote code execution exploit in the Windows Print Spooler service, known as "PrintNightmare", as documented in CVE-2021-34527. After installing this and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system's Trusted Root Certification Authorities trusts signed drivers. Microsoft recommends that you immediately install this update on all supported Windows client and server operating system, starting with devices that currently host the print server role. You also have the option to	KB5004959	N/A

	configure the RestrictDriverInstallationToAdministrators registry setting to prevent non-administrators from installing signed printer drivers on a print server. For more information, see KB5005010.		
Windows Malicious Software Removal Tool - v5.91	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	N/A
2021-07 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This security update includes improvements and fixes that were a part of update KB5003667 (released June 8, 2021) and addresses the following issues: Addresses a remote code execution exploit in the Windows Print Spooler service, known as "PrintNightmare", as documented in CVE-2021-34527. After installing this and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system's Trusted Root Certification Authorities trusts signed drivers. Microsoft recommends that you immediately install this update on all supported Windows client and server operating system, starting with devices that currently host the print server role. You also have the option to configure the	KB5004953	N/A

	RestrictDriverInstallationToAdministrators registry setting to prevent non-administrators from installing signed printer drivers on a print server. For more information, see KB5005010.		
2021-07 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This security update includes quality improvements. Key changes include: Addresses a remote code execution exploit in the Windows Print Spooler service, known as “PrintNightmare”, as documented in CVE-2021-34527. After installing this and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system’s Trusted Root Certification Authorities trusts signed drivers. Microsoft recommends that you immediately install this update on all supported Windows client and server operating system, starting with devices that currently host the print server role. You also have the option to configure the RestrictDriverInstallationToAdministrators registry setting to prevent non-administrators from installing signed printer drivers on a print server. For more information, see KB5005010.	KB5004951	N/A

Windows Malicious Software Removal Tool x64 - v5.91	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers	KB890830	N/A
2021-07 Cumulative Update for Windows Server 2016 for x64-based Systems	This security update includes quality improvements. Key changes include: Removes support for the PerformTicketSignature setting and permanently enables Enforcement mode for CVE-2020-17049. For more information and steps to enable full protection on domain controller servers, see Managing deployment of Kerberos S4U changes for CVE-2020-17049. Addresses an issue that incorrectly renders some Enhanced Metafile Format (EMF) files. This issue occurs if you build the EMF files using third-party applications with ExtCreatePen() and ExtCreateFontIndirect(). Addresses a redirector stop error that is caused by a race condition that occurs when the system deletes binding objects when connections close. Removes the Adobe Flash component from your device. Adds Advanced Encryption Standard (AES) encryption protections for CVE-2021-33757. For more information, see KB5004605. Addresses a vulnerability in which Primary Refresh	KB5004238	N/A

	Tokens are not strongly encrypted. This issue might allow the tokens to be reused until the token expires or is renewed. For more information about this issue, see CVE-2021-33779. Security updates to Windows Apps, Windows Fundamentals, Windows Authentication, Windows User Account Control (UAC), Operating System Security, the Windows Kernel, Windows Graphics, the Microsoft Scripting Engine, the Windows HTML Platforms, the Windows MSHTML Platform, and Windows Active Directory.		

BD Product Name: **BD Pyxis™ CIISafe™**

Date of Critical or Security Patches: July 2021
Abstract: Critical or Security Patches – July 2021

Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for July 2021. These patches were not found to adversely affect BD products and will be applied according to customers' service agreement.

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).

Patch Name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.91 (KB890830)	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	N/A

2021-06 Cumulative Update for .NET Framework 4.8 for Windows Server 2016 for x64 (KB5003542)	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.	KB5003542	N/A
2021-07 Cumulative Update for Windows 10 Version 1607 for x64-based Systems (KB5004948)	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.	KB5004948	N/A
2020-07 Extended Security Updates (ESU) Licensing Preparation Package for Windows 7 for x86-based Systems (KB4575903)	This update provides the complete set of licensing changes to enable installation of the ESU MAK add-on key, which is one of the steps to prepare for installation of Extended Security Updates. (For the full set of steps, please see KB4522133). A reboot is required after installing this update.	KB4575903	N/A
2021-07 Security Monthly Quality Rollup for Windows 7 for x64-based Systems (KB5004289)	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.	KB5004289	N/A

2021-07 Security and Quality Rollup for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows 7 (KB5004229)	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.	KB5004229	N/A
2021-07 Servicing Stack Update for Windows Server 2008 R2 for x64-based Systems (KB5004378)	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.	KB5004378	N/A

BD Product Name: **BD Pyxis™ CUBIE™ Replenishment System**

Date of Critical or Security Patches: July 2021
Abstract: Critical or Security Patches – July 2021

Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for May 2021. These patches were not found to adversely affect BD products and will be applied according to customers' service agreement.

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).

Patch Name	Description	Patch ID	Notes
2020-07 Extended Security Updates (ESU) Licensing Preparation Package for Windows 7 for x86-based Systems (KB4575903)	This update provides the complete set of licensing changes to enable installation of the ESU MAK add-on key, which is one of the steps to prepare for installation of Extended Security Updates. (For the full set of steps, please see KB4522133). A reboot is required after installing this update.	KB4575903	N/A
2021-07 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x64-based Systems (KB500495**3)**	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.	KB5004953	N/A

2021-07 Security Only Quality Update for Windows Embedded Standard 7 for x64-based Systems (KB5004951)	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.	KB5004951	N/A

BD Product Name: **BD Pyxis™ Supply**

Date of Critical or Security Patches: July 2021
Abstract: Critical or Security Patches – July 2021

Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for July 2021. These patches were not found to adversely affect BD products and will be applied according to customers' service agreement.

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).

Patch Name	Description	Patch ID	Notes
2020-12 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems	This security update includes quality improvements like- Security updates to Windows Graphics, Windows Peripherals, and Windows Core Networking.	KB4592495	None
2021-07 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems	This security update includes quality improvements. Key changes include: Addresses a remote code execution exploit in the Windows Print Spooler service, known as "PrintNightmare", as documented in CVE-2021-34527. After installing this and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system's Trusted Root Certification Authorities trusts signed drivers. Microsoft recommends that you	KB5004958	None

	immediately install this update on all supported Windows client and server operating system, starting with devices that currently host the print server role		
2021-07 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems	This security update includes improvements and fixes that were a part of update KB5003671 (released June 8, 2021) and addresses the following issues: Addresses a remote code execution exploit in the Windows Print Spooler service, known as "PrintNightmare", as documented in CVE-2021-34527. After installing this and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system's Trusted Root Certification Authorities trusts signed drivers. Microsoft recommends that you immediately install this update on all supported Windows client and server operating system, starting with devices that currently host the print server role.	KB5004954	None
2021-07 Security Only Quality Update for Windows 7 for x64-based Systems	This security update includes quality improvements. Key changes include: Addresses a remote code execution exploit in the Windows Print Spooler service, known as "PrintNightmare", as documented in CVE-2021-34527. After installing this	KB5004951	None

	and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system's Trusted Root Certification Authorities trusts signed drivers. Microsoft recommends that you immediately install this update on all supported Windows client and server operating system, starting with devices that currently host the print server role.		
2021-07 Security Monthly Quality Rollup for Windows 7 for x64-based Systems	This security update includes improvements and fixes that were a part of update KB5003667 (released June 8, 2021) and addresses the following issues: Addresses a remote code execution exploit in the Windows Print Spooler service, known as "PrintNightmare", as documented in CVE-2021-34527. After installing this and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system's Trusted Root Certification Authorities trusts signed drivers. Microsoft recommends that you immediately install this update on all supported Windows client and server operating system, starting	KB5004953	None

	with devices that currently host the print server role. You also have the option to configure the RestrictDriverInstallationToAdministrators registry setting to prevent non-administrators from installing signed printer drivers on a print server.		
2021-07 Cumulative Update for Windows Server 2016 for x64-based Systems	This security update includes quality improvements. Key changes include: Removes support for the PerformTicketSignature setting and permanently enables Enforcement mode for CVE-2020-17049. For more information and steps to enable full protection on domain controller servers, see Managing deployment of Kerberos S4U changes for CVE-2020-17049. Addresses an issue that incorrectly renders some Enhanced Metafile Format (EMF) files. This issue occurs if you build the EMF files using third-party applications with ExtCreatePen() and ExtCreateFontIndirect(). Addresses a redirector stop error that is caused by a race condition that occurs when the system deletes binding objects when connections close. Removes the Adobe Flash component from your device.	KB5004238	None

	Adds Advanced Encryption Standard (AES) encryption protections for CVE-2021-33757. For more information, see KB5004605. Addresses a vulnerability in which Primary Refresh Tokens are not strongly encrypted. This issue might allow the tokens to be reused until the token expires or is renewed. For more information about this issue, see CVE-2021-33779. Security updates to Windows Apps, Windows Fundamentals, Windows Authentication, Windows User Account Control (UAC), Operating System Security, the Windows Kernel, Windows Graphics, the Microsoft Scripting Engine, the Windows HTML Platforms, the Windows MSHTML Platform, and Windows Active Directory.		
2021-07 Cumulative Update for Windows Server 2016 for x64-based Systems	Addresses a remote code execution exploit in the Windows Print Spooler service, known as “PrintNightmare”, as documented in CVE-2021-34527. After installing this and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system’s Trusted Root Certification Authorities trusts signed drivers.	KB5004948	None

2021-07 Cumulative Update for Windows 10 Version 2004 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) ensure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates. This build includes all the improvements from Windows 10, version 2004.	KB5004945	None
2021-07 Cumulative Update for Windows 10 Version 2004 for x64-based Systems	Updates for verifying usernames and passwords. Updates to improve security when Windows performs basic operations. Updates an issue that might make printing to certain printers difficult. This issue affects various brands and models, but primarily receipt or label printers that connect using a USB port. After installing this update, you do not need to use a Known Issue Rollback (KIR) or a special Group Policy to resolve this issue.	KB5004237	None
2021-07 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 2004 for x64	The July 13, 2021 update for Windows 10, version 2004, Windows Server, version 2004, Windows 10, version 20H2, and Windows Server, version 20H2, and Windows Version 21H1 includes cumulative reliability improvements in .NET Framework 3.5 and 4.8. We recommend that you apply this update as part of your regular maintenance routines.	KB5003537	None
Featured update to Windows 10, version 21H1 by using an enablement package	The enablement package is a great option for installing a scoped feature update like Windows 10, version 21H1 as it enables an update from version 2004 or 20H2 to	KB5000736	None

	version 21H1 with a single restart, reducing update downtime. This enables devices to take advantage of new features now. For version 2004 and 20H2 devices that receive updates directly from Windows Update, devices automatically get the enablement package by installing the feature update to Windows 10, version 21H1.		
Security intelligence updates for Microsoft Defender Antivirus and other Microsoft antimalware	Microsoft continually updates security intelligence in antimalware products to cover the latest threats and to constantly tweak detection logic, enhancing the ability of Microsoft Defender Antivirus and other Microsoft antimalware solutions to accurately identify threats. This security intelligence works directly with cloud-based protection to deliver fast and powerful AI-enhanced, next-generation protection.	KB2267602	None
Remove specific prevalent malware with Windows Malicious Software Removal Tool	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.	KB890830	None

BD Product Name: **BD Pyxis™ Anesthesia ES**

Date of Critical or Security Patches: July 2021

Abstract: Critical or Security Patches – July 2021

Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for July 2021. These patches were not found to adversely affect BD products and will be applied according to customers' service agreement.

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 to smaintain the correct security posture of the system(s).

Patch Name	Description	Patch ID	Notes
2021-07 Cumulative Update for Windows 10 Version 1809 for x86-based Systems	A Security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update form Microsoft. For a complete listing of issues that are included in this update, see the associated Microsoft Knowledge Base article. After install the update, you may have to restart your system.	KB5004947	None
2021-07 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	This security update includes quality improvements. Key changes include: Removes support for the PerformTicketSignature setting and permanently enables Enforcement mode for CVE-2020-17049. For more information and steps to enable full protection on domain controller servers, see Managing deployment of	KB5004238	N/A

	Kerberos S4U changes for CVE-2020-17049. Addresses an issue that incorrectly renders some Enhanced Metafile Format (EMF) files. This issue occurs if you build the EMF files using third-party applications with ExtCreatePen() and ExtCreateFontIndirect(). Addresses a redirector stop error that is caused by a race condition that occurs when the system deletes binding objects when connections close. Removes the Adobe Flash component from your device.		
2021-07 Cumulative Update for .NET Framework 4.8 for Windows 10 Version 1607 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.	KB5004115	N/A
2021-07 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	Addresses a remote code execution exploit in the Windows Print Spooler service, known as "PrintNightmare", After installing this and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system's Trusted Root Certification Authorities trusts signed drivers.	KB5004948	N/A

BD Product Name: **BD Pyxis™ CIISafe ES**

Date of Critical or Security Patches: July 2021

Abstract: Critical or Security Patches – July 2021

Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for July 2021. These patches were not found to adversely affect BD products and will be applied according to customers' service agreement.

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 to smaintain the correct security posture of the system(s).

Patch Name	Description	Patch ID	Notes
2021-07 Cumulative Update for Windows 10 Version 1809 for x86-based Systems	A Security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update form Microsoft. For a complete listing of issues that are included in this update, see the associated Microsoft Knowledge Base article. After install the update, you may have to restart your system.	KB5004947	None
Security Update for SQL Server 2016 Service Pack 2 CU	Security issues have been identified in the SQL Server 2016 Service Pack 2 CU that could allow an attacker to compromise your system and gain control over it. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer.	KB4583461	None

BD Product Name: **BD Pyxis™ Med Station ES**

Date of Critical or Security Patches: July 2021

Abstract: Critical or Security Patches – July 2021

Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for July 2021. These patches were not found to adversely affect BD products and will be applied according to customers' service agreement.

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).

Patch Name	Description	Patch ID	Notes
2021-07 Cumulative Update for Windows 10 Version 1809 for x86-based Systems	A Security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update form Microsoft. For a complete listing of issues that are included in this update, see the associated Microsoft Knowledge Base article. After install the update, you may have to restart your system.	KB5004947	N/A
2021-07 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems	This security update includes improvements and fixes that were a part of update KB5004954 (released July 6, 2021) and addresses the following issues: • Addresses an issue in which 16-bit applications fail with an error message that states a general fault in VBRUN300.DLL	KB5004298	N/A

	- Addresses an issue in which some EMFs built by using third-party applications that use ExtCreatePen and ExtCreateFontIndirect render incorrectly - Adds Advanced Encryption Standard (AES) encryption protections		
2021-07 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems	This security update includes improvements and fixes that were a part of update KB5003671 (released June 8, 2021)	KB5004954	N/A
2021-07 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems	This security update includes quality improvements. Key changes include: Addresses a remote code execution exploit in the Windows Print Spooler service, known as "PrintNightmare". After installing this and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system's Trusted Root Certification Authorities trusts signed drivers.	KB5004958	N/A
Windows Malicious Software Removal Tool x64 - v5.91 (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	KB890830	N/A

	Windows 8.1 Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2 Windows 7 Windows Server 2008		
2021-07 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This security update includes quality improvements. Key changes include: Addresses a remote code execution exploit in the Windows Print Spooler service, known as "PrintNightmare", as documented in CVE-2021-34527. After installing this and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system's Trusted Root Certification Authorities trusts signed drivers. Microsoft recommends that you immediately install this update on all supported Windows client and server operating system, starting with devices that currently host the print server role. You also have the option to configure the RestrictDriverInstallationToAdministrators registry setting to prevent non-administrators from installing signed printer drivers on a print server. For more information, see KB5005010	KB5004951	N/A

Patch Name	Description	Patch ID	Notes
2021-07 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This security update includes improvements and fixes that were a part of update KB5003667 (released June 8, 2021) and addresses the following issues: Addresses a remote code execution exploit in the Windows Print Spooler service, known as "PrintNightmare", as documented in CVE-2021-34527. After installing this and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system's Trusted Root Certification Authorities trusts signed drivers. Microsoft recommends that you immediately install this update on all supported Windows client and server operating system, starting with devices that currently host the print server role. You also have the option to configure the RestrictDriverInstallationToAdministrators registry setting to prevent non-administrators from installing signed printer drivers on a print server. For more information, see KB5005010.	KB5004953	N/A

2021-07 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	Addresses a remote code execution exploit in the Windows Print Spooler service, known as “PrintNightmare”, After installing this and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system’s Trusted Root Certification Authorities trusts signed drivers.	KB5004948	N/A
2021-07 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5004954)	This security update includes improvements and fixes that were a part of update KB5003671 (released June 8, 2021) and addresses the following issues: Addresses a remote code execution exploit in the Windows Print Spooler service, known as “PrintNightmare”, as documented in CVE-2021-34527.	KB5004954	N/A
2021-07 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5004958)	This security update includes quality improvements. Key changes include: Addresses a remote code execution exploit in the Windows Print Spooler service, known as “PrintNightmare”, as documented in CVE-2021-34527.	KB5004958	N/A
2021-07 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	This security update includes quality improvements. Key changes include:	KB5004238	N/A

	Removes support for the PerformTicketSignature setting and permanently enables Enforcement mode for CVE-2020-17049. For more information and steps to enable full protection on domain controller servers, see Managing deployment of Kerberos S4U changes for CVE-2020-17049. Addresses an issue that incorrectly renders some Enhanced Metafile Format (EMF) files. This issue occurs if you build the EMF files using third-party applications with ExtCreatePen() and ExtCreateFontIndirect(). Addresses a redirector stop error that is caused by a race condition that occurs when the system deletes binding objects when connections close. Removes the Adobe Flash component from your device.		
2021-07 Cumulative Update for .NET Framework 4.8 for Windows 10 Version 1607 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.	**KB5004115**	N/A

BD Product Name: **BD Pyxis® PARx**

Date of Critical or Security Patches: July 2021
Abstract: Critical or Security Patches – July 2021
Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for July 2021. These patches were not found to adversely affect BD products and will be applied according to customers' service agreement.

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).

Patch Name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.91 (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	KB890830	N/A
2021-07 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	Addresses a remote code execution exploit in the Windows Print Spooler service, known as "PrintNightmare", After installing this and later Windows updates, users who are not administrators can only install signed print drivers to a print server. By default, administrators can install signed and unsigned printer drivers to a print server. The installed root certificates in the system's Trusted Root Certification Authorities trusts signed drivers.	KB5004948	N/A

BD Product Name: **BD Pyxis® Connect**

Date of Critical or Security Patches: June 2021
Abstract: Critical or Security Patches – June 2021

Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for July 2021. These patches were not found to adversely affect BD products and will be applied according to customers' service agreement.

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).

Patch Name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.91 (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	KB890830	N/A
Security Intelligence Update for Windows Defender Antivirus Version 1.343.1673.0	Microsoft works to help make computing as secure as possible for our customers. As part of this effort, Microsoft Windows Defender regularly downloads updates to the definition files that are used to identify spyware and other potentially unwanted software.	KB915597	N/A

BD Product Name: **BD Pyxis™ IV Prep**

Date of Critical or Security Patches: July 2021
Abstract: Critical or Security Patches – July 2021

Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for July 2021. These patches were not found to adversely affect BD products and will be applied according to customers' service agreement.

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).

Patch Name	Description	Patch ID	Notes
2021-07 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.	KB5004238	None
Windows Malicious Software Removal Tool x64 - v5.90	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	KB890830	None
2021-07 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	KB5004948	None

2021-07 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.	KB5004958	None
2021-07 Security and Quality Rollup for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 for x64	Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.	KB5004231	None
2021-07 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, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5004298	None
2020-12 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	KB4592495	None

2021-07 Security and Quality Rollup for .NET Framework 4.8 for Windows Server 2012 R2 for x64	Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.	KB5004118	None