Security Patches:
BD Pyxis™ Anesthesia Station 4000

August 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for August 2023. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.116	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	N/A
2023-08 Cumulative Update for Windows Server 2016 for x64-based Systems	This security update includes quality improvements. When you install this KB: ▪ This update addresses an issue that affects Kerberos constrained delegation (KCD). It fails on read-write domain controllers. The error message is, "KRB_AP_ERR_MODIFIED." This occurs after you install the November 2022 security updates.	KB5029242	N/A
2023-08 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5028240 (released July 11, 2023). This update also makes improvements for the following issue: ▪ Kerberos constrained delegation (KCD) might fail with the error message KRB_AP_ERR_MODIFIED on read/write domain controllers after installing the November 2022 security updates.	KB5029296	N/A
2023-08 Security and Quality Rollup for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5029651	N/A

2023-08 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems	This security update resolves vulnerabilities in Internet Explorer.	KB5029243	N/A
2023-08 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This update makes improvements for the following issue: ▪ Kerberos constrained delegation (KCD) might fail with the error message KRB_AP_ERR_MODIFIED on read/write domain controllers after installing the November 2022 security updates.	KB5029307	N/A
2023-08 Security Only Update for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7	CVE-2023-36899 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in applications on IIS using their parent application's Application Pool which can lead to privilege escalation or other security bypasses. For more information see CVE 2023-36899. CVE-2023-36873 - .NET Framework Spoofing Vulnerability This security update addresses a vulnerability where unauthenticated remote attacker can sign ClickOnce deployments without a valid code signing certificate. For more information see CVE-2023-36873.	KB5029566	N/A

Security Patches: BD Pyxis™ C^II^Safe

August 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for August 2023. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
2023-08 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems (KB 5029296)	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.	KB5029296	N/A
2023-08 Security and Quality Rollup for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7 (KB5029651)	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.	KB5029651	N/A
2023-08 Cumulative Update for Windows 10 Version 1607 for x64-based Systems (KB5029242)	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.	KB5029242	N/A
2023-08 Cumulative Update for .NET Framework 4.8 for Windows 10 Version 1607 for x64 (KB5028952)	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.	KB5028952	N/A

Windows Malicious Software Removal Tool - v5.116 (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

Security Patches:
BD Pyxis™ MedStation™ 4000

August 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for August 2023. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.116	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	N/A
2023-08 Cumulative Update for Windows Server 2016 for x64-based Systems	This security update includes quality improvements. When you install this KB: ▪ This update addresses an issue that affects Kerberos constrained delegation (KCD). It fails on read-write domain controllers. The error message is, "KRB_AP_ERR_MODIFIED." This occurs after you install the November 2022 security updates.	KB5029242	N/A
2023-08 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	This security update includes quality improvements. When you install this KB: ▪ This update addresses an issue that affects Kerberos constrained delegation (KCD). It fails on read-write domain controllers. The error message is, "KRB_AP_ERR_MODIFIED." This occurs after you install the November 2022 security updates.	KB5029242	N/A
Windows Malicious Software Removal Tool - v5.116	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	N/A
2023-08 Security Only Quality Update for Windows Server 2008 for x86-based Systems	This update makes improvements for the following issue: ▪ Kerberos constrained delegation (KCD) might fail with the error message KRB_AP_ERR_MODIFIED on read/write domain controllers after installing the November 2022 security updates.	KB5029301	N/A

2023-08 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	**This cumulative security update contains improvements that are part of update KB5028240 (released July 11, 2023). This update also makes improvements for the following issue:** ▪ Kerberos constrained delegation (KCD) might fail with the error message KRB_AP_ERR_MODIFIED on read/write domain controllers after installing the November 2022 security updates.	KB5029296	**N/A**
2023-08 Security and Quality Rollup for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5029651	N/A
2023-08 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems	This security update resolves vulnerabilities in Internet Explorer.	KB5029243	N/A
2023-08 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This update makes improvements for the following issue: ▪ Kerberos constrained delegation (KCD) might fail with the error message KRB_AP_ERR_MODIFIED on read/write domain controllers after installing the November 2022 security updates.	KB5029307	N/A
2023-08 Security Only Update for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7	CVE-2023-36899 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in applications on IIS using their parent application's Application Pool which can lead to privilege escalation or other security bypasses. For more information see CVE 2023-36899. CVE-2023-36873 - .NET Framework Spoofing Vulnerability This security update addresses a vulnerability where unauthenticated remote attacker can sign ClickOnce deployments without a valid code signing certificate. For more information see CVE-2023-36873.	KB5029566	N/A
2023-08 Security Monthly Quality Rollup for Windows Server 2008 for x86-based Systems	This cumulative security update contains improvements that are part of update KB5028222 (released July 11, 2023).	KB5029318	N/A

Security Patches: Security Module

August 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for August 2023. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.116 (KB890830)	After the download, this tool runs one time to check the 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. This tool is not a replacement for an antivirus product.	KB890830	N/A
2023-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5029312)	This cumulative security update includes improvements that are part of update KB5028228 (released July 11, 2023). This update also makes improvements for the following issue: Kerberos constrained delegation (KCD) might fail with the error message KRB_AP_ERR_MODIFIED on read/write domain controllers after installing the November 2022 security updates.	KB5029312	N/A
2023-08 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems (KB5029243)	The improvements that are included in this Internet Explorer update are also included in the August 2023 Monthly Rollup. Installing either this Internet Explorer update or the Monthly Rollup installs the same improvements.	KB5029243	N/A
2023-08 Security and Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 for x64 (KB5029653)	• CVE-2023-36899 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in applications on IIS using their parent application's Application Pool which can lead to privilege escalation or other security bypasses. • CVE-2023-36873 - .NET Framework Spoofing Vulnerability This security update addresses a vulnerability where unauthenticated remote attacker can sign ClickOnce deployments without a valid code signing certificate.	KB5029653	N/A

2023-08 Security Only Update 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 (KB5029568)	• CVE-2023-36899 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in applications on IIS using their parent application's Application Pool which can lead to privilege escalation or other security bypasses. • CVE-2023-36873 - .NET Framework Spoofing Vulnerability This security update addresses a vulnerability where unauthenticated remote attacker can sign ClickOnce deployments without a valid code signing certificate.	KB5029568	N/A
2023-08 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5029304)	This security update includes following improvements: Kerberos constrained delegation (KCD) might fail with the error message KRB_AP_ERR_MODIFIED on read/write domain controllers after installing the November 2022 security updates.	KB5029304	N/A
2023-08 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB5029368)	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.	KB5029368	N/A
2023-08 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5029242)	This update addresses an issue that affects Kerberos constrained delegation (KCD). It fails on read-write domain controllers. The error message is, "KRB_AP_ERR_MODIFIED." This occurs after you install the November 2022 security updates.	KB5029242	N/A

Security Patches: BD Pyxis™ IV Prep

August 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for August 2023. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
2023-08 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5029242)	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.	KB5029242	N/A
Windows Malicious Software Removal Tool x64 - v5.116 (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

2023-08 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB5029368)	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.	KB5029368	N/A
2023-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5029312)	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.	KB5029312	N/A
2023-08 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems (KB5029243)	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.	KB5029243	N/A
2023-08 Security and Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 for x64 (KB5029653)	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.	KB5029653	N/A
2023-08 Security Only Update 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 (KB5029568)	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.	KB5029568	N/A

2023-08 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5029304)	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.	KB5029304	N/A

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

bd.com

Security Patches: BD Pyxis™ Connect

August 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for August 2023. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
2023-08 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB5029368)	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.	KB5029368	N/A
2023-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5029312)	This cumulative security update includes improvements that are part of update KB5028228 (released July 11, 2023). This update also makes improvements for the following issue: • Kerberos constrained delegation (KCD) might fail with the error message KRB_AP_ERR_MODIFIED on read/write domain controllers after installing the November 2022 security updates.	KB5029312	N/A
Windows Malicious Software Removal Tool x64 - v5.115 (KB890830)	Windows Malicious Software Removal Tool (MSRT) helps keep Windows computers free from prevalent malware. MSRT finds and removes threats and reverses the changes made by these threats. MSRT is generally released monthly as part of Windows Update or as a standalone tool.	KB890830	N/A

2023-08 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems (KB5029243)	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 Server 2012 • Internet Explorer 11 on Windows Server 2008 R2 SP1 • Internet Explorer 9 on Windows Server 2008 SP2	KB5029243	N/A
2023-08 Security and Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 for x64 (KB5029653)	This update addresses the following .Net Framework related vulnerabilities: • CVE-2023-36899 - .NET Framework Remote Code Execution Vulnerability: This security update addresses a vulnerability in applications on IIS using their parent application's Application Pool which can lead to privilege escalation or other security bypasses. • CVE-2023-36873 - .NET Framework Spoofing Vulnerability: This security update addresses a vulnerability where unauthenticated remote attacker can sign ClickOnce deployments without a valid code signing certificate.	KB5029653	N/A
2023-08 Security Only Update 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 (KB5029568)	This update addresses the following .Net Framework related vulnerabilities: • CVE-2023-36899 - .NET Framework Remote Code Execution Vulnerability: This security update addresses a vulnerability in applications on IIS using their parent application's Application Pool which can lead to privilege escalation or other security bypasses. • CVE-2023-36873 - .NET Framework Spoofing Vulnerability: This security update addresses a vulnerability where unauthenticated remote attacker can sign ClickOnce deployments without a valid code signing certificate.	KB5029568	N/A
2023-08 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5029304)	This update makes improvements for the following issue: • Kerberos constrained delegation (KCD) might fail with the error message KRB_AP_ERR_MODIFIED on read/write domain controllers after installing the November 2022 security updates.	KB5029304	N/A

2023-08 Cumulative Security Update for Windows 10 Version 22H2 for x64-based Systems (KB5029244)	This update addresses security issues for your Windows operating system.	KB5029244	N/A
2023-08 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5029242)	This security update includes quality improvements. When you install this KB: • This update addresses an issue that affects Kerberos constrained delegation (KCD). It fails on read-write domain controllers. The error message is, “KRB_AP_ERR_MODIFIED.” This occurs after you install the November 2022 security updates.	KB5029242	N/A
2023-08 Cumulative Update for .NET Framework 4.8 for Windows Server 2016 for x64 (KB5028952)	This update includes the following Quality and Reliability improvements: • WPF - Addresses an issue where XPS documents using LinkTarget aren't rendering properly. • Networking- Addresses an issue where using proxy with continuous load may lead to memory leak resulting in high memory usage, or potentially OutOfMemoryException.	KB5028952	N/A
2023-08 Cumulative Security Update for .NET Framework 3.5,4.8, 4.8.1 for Windows 10 Version 22H2 for x64 (KB5029649)	This security update addresses a vulnerability in applications on IIS using their parent application's Application Pool which can lead to privilege escalation or other security bypasses.	KB5029649	N/A

Security Patches: BD Pyxis^{TM} Logistics

August 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for August 2023. These patches were not found to adversely affect BD Pharmogistics products and will be applied according to customers' service agreements.

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

Microsoft® patches

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

2023-08 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5029242)	Improvements This security update includes quality improvements. When you install this KB: This update addresses an issue that affects Kerberos constrained delegation (KCD). It fails on read-write domain controllers. The error message is, “KRB_AP_ERR_MODIFIED.” This occurs after you install the November 2022 security updates. If you installed earlier updates, only the new updates contained in this package will be downloaded and installed on your device.	KB5029242	N/A
2023-08 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB5029368) Last Modified: 8/8/2023	Summary 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.	KB5029368	N/A

2023-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5029312) Last Modified: 8/8/2023	Summary Learn more about this cumulative security update, including improvements, any known issues, and how to get the update. Improvements This cumulative security update includes improvements that are part of update KB5028228 (released July 11, 2023). This update also makes improvements for the following issue: Kerberos constrained delegation (KCD) might fail with the error message KRB_AP_ERR_MODIFIED on read/write domain controllers after installing the November 2022 security updates.	KB5029312	N/A
2023-08 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems (KB5029243) Last Modified: 8/8/2023	Summary This security update resolves vulnerabilities in Internet Explorer. To learn more about these vulnerabilities, see Deployments I Security Update Guide.	KB5029243	N/A
2023-08 Security and Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 for x64 (KB5029653) Last Modified: 8/8/2023	Summary Security Improvements CVE-2023-36899 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in applications on IIS using their parent application's Application Pool which can lead to privilege escalation or other security bypasses. For more information see CVE 2023-36899. CVE-2023-36873 - .NET Framework Spoofing Vulnerability This security update addresses a vulnerability where unauthenticated remote attacker can sign ClickOnce deployments without a valid code signing certificate. For more information see CVE-2023-36873. Quality and Reliability Improvements	KB5029653	N/A

	For a list of improvements that were released with this update, please see the article links in the Additional Information section of this article.		
2023-08 Security Only Update 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 (KB5029568) Last Modified: 8/8/2023	Summary CVE-2023-36899 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in applications on IIS using their parent application’s Application Pool which can lead to privilege escalation or other security bypasses. For more information see CVE 2023-36899. CVE-2023-36873 - .NET Framework Spoofing Vulnerability This security update addresses a vulnerability where unauthenticated remote attacker can sign ClickOnce deployments without a valid code signing certificate. For more information see CVE-2023-36873.	KB5029568	N/A
2023-08 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5029304) Last Modified: 8/8/2023	Summary Learn more about this security-only update, including improvements, any known issues, and how to get the update. Improvements This update makes improvements for the following issue: Kerberos constrained delegation (KCD) might fail with the error message KRB_AP_ERR_MODIFIED on read/write domain controllers after installing the November 2022 security updates. For more information about the resolved security vulnerabilities, please refer to the Deployments I Security Update Guide and the August 2023 Security Updates.	KB5029304	N/A

2023-08 Security Only Quality Update for Windows Server 2008 R2 for x64-based Systems (KB5029307) Last Modified: 8/8/2023	Summary Learn more about this security-only update, including improvements, any known issues, and how to get the update. Improvements This update makes improvements for the following issue: Kerberos constrained delegation (KCD) might fail with the error message KRB_AP_ERR_MODIFIED on read/write domain controllers after installing the November 2022 security updates	KB5029307	N/A
2023-08 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (KB5029296) Last Modified: 8/8/2023	Summary Learn more about this cumulative security update, including improvements, any known issues, and how to get the update. Improvements This cumulative security update contains improvements that are part of update KB5028240 (released July 11, 2023). This update also makes improvements for the following issue: Kerberos constrained delegation (KCD) might fail with the error message KRB_AP_ERR_MODIFIED on read/write domain controllers after installing the November 2022 security updates.	KB5029296	N/A
2023-08 Cumulative Security Update for Internet Explorer 11 for Windows Server 2008 R2 for x64-based systems (KB5029243) Last Modified: 8/8/2023	Summary This security update resolves vulnerabilities in Internet Explorer. To learn more about these vulnerabilities, see Deployments I Security Update Guide.	KB5029243	N/A

2023-08 Cumulative Update for Windows 10 Version 22H2 for x64-based Systems (KB5029244) Last Modified: 8/8/2023	Improvements Windows 10 servicing stack update - 19044.3266 and 19045.3266 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.	KB5029244	N/A
2023-08 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2 for x64 (KB5029649) Last Modified: 8/8/2023	Summary This article describes the security and Cumulative Update for 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2. Security Improvements CVE-2023-36899 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in applications on IIS using their parent application's Application Pool which can lead to privilege escalation or other security bypasses. For more information see CVE 2023-36899. CVE-2023-36873 - .NET Framework Spoofing Vulnerability This security update addresses a vulnerability where unauthenticated remote attacker can sign ClickOnce deployments without a valid code signing certificate. For more information see CVE-2023-36873. Quality and Reliability Improvements For a list of improvements that were released with this update, please see the article links in the Additional Information section of this article.	KB5029649	N/A

Microsoft .NET Framework 4.8.1 for Windows 10 Version 22H2 for x64 (KB5011048) Last Modified: 8/8/2023	Microsoft .NET Framework 4.8.1 for Windows 10 version 21H2, Windows 10 version 22H2, Windows 11 version 21H2, Windows Server 2022 (Desktop, Azure Editions), Azure Stack 21H2 and Azure Stack 22H2 (KB5011048) Note: NET Framework 4.8.1 installers have been refreshed to include the latest servicing updates as of June 13th, 2023. Apart from the servicing fixes, there is no change in the .NET Framework 4.8.1 product that was released originally on August 9th, 2022. If you have already installed .NET Framework 4.8.1, you do not need to install this update. Microsoft .NET Framework 4.8.1 is a highly compatible and in-place update to .NET Framework 4.8. It includes native support for the Arm64 architecture (Windows 11+), accessibility improvements as well as other improvements. For a complete list of improvements see: .NET Framework 4.8.1 release notes. Microsoft .NET Framework 4.8.1 is available on Windows Update and Microsoft Update Catalog. It will be offered as a recommended update on Windows Update on applicable configurations.	KB5011048	N/A
2023-08 Cumulative Update for Windows Server 2019 for x64-based Systems (KB5029247) Last Modified: 8/8/2023	Improvements This security update includes improvements. When you install this KB: This update addresses an issue that affects apps that use DirectX on older Intel graphics drivers. You might receive an error from apphelp.dll. This update affects user mode printer drivers. They unload unexpectedly. This occurs when you print from multiple print queues to the same printer driver. This update affects the Windows Kernel Vulnerable Driver Blocklist, DriverSiPolicy.p7b. It adds drivers that are at risk for Bring Your Own Vulnerable Driver (BYOVD) attacks. This update addresses an issue that affects Kerberos constrained delegation (KCD). It fails on read-write domain controllers. The error message is, “KRB_AP_ERR_MODIFIED.” This occurs after you install the November 2022 security updates.	KB5029247	N/A

2023-08 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 (KB5029647) Last Modified: 8/8/2023	Summary This article describes the security and Cumulative Update for 3.5, 4.7.2 and 4.8 for Windows 10, version 1809 and Windows Server 2019. Security Improvements CVE-2023-36899 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in applications on IIS using their parent application's Application Pool which can lead to privilege escalation or other security bypasses. For more information see CVE 2023-36899. CVE-2023-36873 - .NET Framework Spoofing Vulnerability This security update addresses a vulnerability where unauthenticated remote attacker can sign ClickOnce deployments without a valid code signing certificate. For more information see CVE-2023-36873.	KB5029647	N/A

Security Patches: BD Pyxis™ PARx™

August 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for August 2023. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.116	Windows Malicious Software Removal Tool (MSRT) 5.116 helps remove malicious software from computers running Windows11, Windows 10, Windows 8.1, Windows Server 2012 R2, Windows 8, Windows Server 2012, Windows 7, or Windows Server 2008.	KB890830	N/A
2023-08 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	The remote Windows host is missing security update 5029242. It is, therefore, affected by multiple vulnerabilities - Microsoft Message Queuing Remote Code Execution Vulnerability (CVE-2023-35385, CVE-2023-36910, CVE-2023-36911) - Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability (CVE-2023-36882) - Windows Bluetooth A2DP driver Elevation of Privilege Vulnerability (CVE-2023-35387) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.	KB5029242	N/A

2023-08 Cumulative Security Update for Internet Explorer 11 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.	KB5029243	N/A
2023-08 Security and Quality Rollup for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5029651	N/A
2023-08 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	The Microsoft Security Response Center (MSRC) investigates all reports of security vulnerabilities affecting Microsoft products and services, and provides the information here as part of the ongoing effort to help you manage security risks and help keep your systems protected.	KB5029296	N/A
2023-08 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	The remote Windows host is missing security update 5029307. It is, therefore, affected by multiple vulnerabilities - Microsoft Message Queuing Remote Code Execution Vulnerability (CVE-2023-35385, CVE-	KB5029307	N/A

	2023-36910, CVE-2023-36911) - Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability (CVE-2023-36882) - Windows Fax Service Remote Code Execution Vulnerability (CVE-2023-35381)		
2023-08 Security Only Update for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5029566	N/A

Security Patches:
BD Pyxis™ Tissue & Implant Management System

August 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for August 2023. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
2023-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems	This cumulative security update includes improvements that are part of update KB5028228 (released July 11, 2023). This update also makes improvements for the following issue: Kerberos constrained delegation (KCD) might fail with the error message KRB_AP_ERR_MODIFIED on read/write domain controllers after installing the November 2022 security updates. For more information about the resolved security vulnerabilities, please refer to the Deployments I Security Update Guide and the August 2023 Security Updates.	KB5029312	N/A
2023-08 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems	The improvements that are included in this Internet Explorer update are also included in the August 2023 Monthly Rollup. Installing either this Internet Explorer update or the Monthly Rollup installs the same improvements. This update is not applicable for installation on a device on which the Monthly Rollup from August 2023 (or a later month) is already installed. This is because that update contains all the same improvements that are included in this Internet Explorer update.	KB5029243	N/A

	If you use update management processes other than Windows Update and you automatically approve all security update classifications for deployment, this update, the August 2023 Security-Only Update, and the August 2023 Monthly Rollup are deployed. We recommend that you review your update deployment rules to make sure that the desired updates are deployed. If you install a language pack after you install this update, you must reinstall this update. Therefore, we recommend that you install any language packs that you need before you install this update. For more information, see Add language packs to Windows. This security update resolves vulnerabilities in Internet Explorer. To learn more about these vulnerabilities, see Deployments I Security Update Guide. Additionally, see the following articles for more information about cumulative updates: Windows Server 2008 SP2 update history Windows 7 SP1 and Windows Server 2008 R2 SP1 update history Windows Server 2012 update history Windows 8.1 and Windows Server 2012 R2 update history		
2023-08 Security and Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 for x64	CVE-2023-36899 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in applications on IIS using their parent application's Application Pool which can lead to privilege escalation or other security bypasses. For more information see CVE 2023-36899. CVE-2023-36873 - .NET Framework Spoofing Vulnerability This security update addresses a vulnerability where unauthenticated remote attacker can sign ClickOnce deployments without a valid code signing certificate. For more information see CVE-2023-36873. Quality and Reliability Improvements	KB5029653	N/A

	For a list of improvements that were released with this update, please see the article links in the Additional Information section of this article.		
Windows Malicious Software Removal Tool x64 - v5.115	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers that are running any of the following operating systems: Windows 10 Windows Server 2019 Windows Server 2016 Windows 8.1 Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2 Windows 7 Windows Server 2008 Microsoft releases the MSRT on a monthly cadence as part of Windows Update or as a standalone tool. Use this tool to find and remove specific prevalent threats and reverse the changes they have made (see covered malware families). For comprehensive malware detection and removal, consider using Windows Defender Offline or Microsoft Safety Scanner. This article contains information about how the tool differs from an antivirus or antimalware product, how you can download and run the tool, what happens when the tool finds malware, and tool release information. It also includes information for the administrators and advanced users, including information about supported command-line switches.	KB890830	N/A

2023-08 Security Only Update 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	CVE-2023-36899 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in applications on IIS using their parent application's Application Pool which can lead to privilege escalation or other security bypasses. For more information see CVE 2023-36899. CVE-2023-36873 - .NET Framework Spoofing Vulnerability This security update addresses a vulnerability where unauthenticated remote attacker can sign ClickOnce deployments without a valid code signing certificate. For more information see CVE-2023-36873.	KB5029568	N/A
2023-08 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems	This update makes improvements for the following issue: Kerberos constrained delegation (KCD) might fail with the error message KRB_AP_ERR_MODIFIED on read/write domain controllers after installing the November 2022 security updates. For more information about the resolved security vulnerabilities, please refer to the Deployments I Security Update Guide and the August 2023 Security Updates.	KB5029304	N/A
2023-08 Cumulative Update for Windows Server 2016 for x64-based Systems	This security update includes quality improvements. When you install this KB: This update addresses an issue that affects Kerberos constrained delegation (KCD). It fails on read-write domain controllers. The error message is, "KRB_AP_ERR_MODIFIED." This occurs after you install the November 2022 security updates. If you installed earlier updates, only the new updates contained in this package will be downloaded and installed on your device. For more information about security vulnerabilities, please refer to the new Security Update Guide website and the August 2023 Security Updates.	KB5029242	N/A

2023-08 Cumulative Update for .NET Framework 4.8 for Windows Server 2016 for x64	CVE-2023-36899 - .NET Framework Remote Code Execution Vulnerability This security update addresses a vulnerability in applications on IIS using their parent application’s Application Pool which can lead to privilege escalation or other security bypasses. For more information see CVE 2023-36899. CVE-2023-36873 - .NET Framework Spoofing Vulnerability This security update addresses a vulnerability where unauthenticated remote attacker can sign ClickOnce deployments without a valid code signing certificate. For more information see CVE-2023-36873. Quality and Reliability Improvements WPF - Addresses an issue where XPS documents using LinkTarget aren't rendering properly. Networking - Addresses an issue where using proxy with continuous load may lead to memory leak resulting in high memory usage, or potentially OutOfMemoryException. *Windows Presentation Foundation (WPF)	KB5028952	N/A
2023-08 Servicing Stack Update for Windows Server 2012 R2 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.	KB5029368	N/A

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

August 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for August 2023. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
2023-08 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5029307	N/A
2023-08 Security Only Update for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5029566	N/A

Windows Malicious Software Removal Tool x64 - v5.116	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**
2023-08 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5029243	N/A
2023-08 Security and Quality Rollup for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5029651	N/A
2023-08 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5029296	N/A
2023-08 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.	KB5029242	N/A

2023-08 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 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.	KB5029247	**N/A**
2023-08 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10 Version 1809 for x64	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5029647	N/A
2023-08 Cumulative Update for Windows 10 Version 21H2 for x64-based Systems	Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.	KB5029244	N/A
2023-08 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 21H2 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.	KB5029648	N/A

Security Patches:
BD Pyxis™ CII Safe ES

August 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for August 2023. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.116	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
2023-08 Cumulative Update for Windows 10 Version 21H2 for x64-based Systems	Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.	KB5029244	N/A

2023-08 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 21H2 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.	KB5029648	N/A

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

August 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for August 2023. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
2023-08 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5029307	N/A
2023-08 Security Only Update for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5029566	N/A

Windows Malicious Software Removal Tool x64 - v5.116	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
2023-08 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5029243	N/A
2023-08 Security and Quality Rollup for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5029651	N/A
2023-08 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5029296	N/A
2023-08 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.	KB5029242	N/A

2023-08 Cumulative Update for .NET Framework 4.8 for Windows 10 Version 1607 for x64	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5028952	N/A
2023-08 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 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.	KB5029247	N/A
2023-08 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10 Version 1809 for x64	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5029647	N/A
2023-08 Cumulative Update for Windows 10 Version 21H2 for x64-based Systems	Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.	KB5029244	N/A
2023-08 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 21H2 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.	KB5029648	N/A

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

August 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for August 2023. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
2023-08 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.	KB5029368	N/A
2023-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5029312	N/A

2023-08 Cumulative Security Update for Internet Explorer 11 for Windows Server 2008 R2 for x64-based systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5029243	N/A
2023-08 Security and Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 for x64	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.	KB5029653	N/A
2023-08 Security Only Update 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.	KB5029568	N/A
Windows Malicious Software Removal Tool x64 - v5.116	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

2023-08 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.	KB5029304	N/A
2023-08 Security Only Quality Update for Windows Server 2008 for x86-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5029301	N/A
2023-08 Security Monthly Quality Rollup for Windows Server 2008 for x64-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5029318	N/A
2023-08 Cumulative Update for Windows Server 2016 for x64-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5029242	N/A

2023-08 Cumulative Update for Windows Server 2019 for x64-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5029247	N/A
2023-08 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 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.	KB5029647	N/A
2021-08 Servicing Stack Update for Windows Server 2019 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.	KB5005112	N/A

Security Patches:

BD Pyxis™ SupplyStation™

Aug 2023

BD has identified patches from Microsoft® that have been identified as critical or security related for August 2023. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
2023-08 Security Only Quality Update for Windows Server 2008 for x86-based Systems (KB5029301)	This update makes improvements for the following issue: • Kerberos constrained delegation (KCD) might fail with the error message KRB_AP_ERR_MODIFIED on read/write domain controllers after installing the November 2022 security updates. For more information about the resolved security vulnerabilities, please refer to the Deployments I Security Update Guide and the August 2023 Security Updates.	KB5029301	N/A
2023-08 Security Monthly Quality Rollup for Windows Server 2008 for x86-based Systems (KB5029318)	This cumulative security update contains improvements that are part of update KB5028222 (released July 11, 2023). This update also makes improvements for the following issue: • Kerberos constrained delegation (KCD) might fail with the error message KRB_AP_ERR_MODIFIED on read/write domain controllers after installing the November 2022 security updates. For more information about the resolved security vulnerabilities, please refer to the Deployments I Security Update Guide and the August 2023 Security Updates.	KB5029318	N/A
2023-08 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems (KB5029296)	This cumulative security update contains improvements that are part of update KB5028240 (released July 11, 2023). This update also makes improvements for the following issue: • Kerberos constrained delegation (KCD) might fail with the error message KRB_AP_ERR_MODIFIED on read/write domain controllers after installing the November 2022 security updates.	KB5029296	N/A

	For more information about the resolved security vulnerabilities, please refer to the Deployments I Security Update Guide and the August 2023 Security Updates.		
2023-08 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems (KB5029307)	This update makes improvements for the following issue: • Kerberos constrained delegation (KCD) might fail with the error message KRB_AP_ERR_MODIFIED on read/write domain controllers after installing the November 2022 security updates. For more information about the resolved security vulnerabilities, please refer to the Deployments I Security Update Guide and the August 2023 Security Updates.	KB5029307	N/A
2023-08 Security Only Update for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7 (KB5029566)	CVE-2023-36899 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in applications on IIS using their parent application's Application Pool which can lead to privilege escalation or other security bypasses. For more information see CVE 2023-36899. CVE-2023-36873 - .NET Framework Spoofing Vulnerability • This security update addresses a vulnerability where unauthenticated remote attacker can sign ClickOnce deployments without a valid code signing certificate. For more information see CVE-2023-36873.	KB5029566	N/A
2023-08 Security and Quality Rollup for .NET Framework 3.5.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Embedded Standard 7 (KB5029651)	CVE-2023-36899 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in applications on IIS using their parent application's Application Pool which can lead to privilege escalation or other security bypasses. For more information see CVE 2023-36899. CVE-2023-36873 - .NET Framework Spoofing Vulnerability • This security update addresses a vulnerability where unauthenticated remote attacker can sign ClickOnce deployments without a valid code signing certificate. For more information see CVE-2023-36873.	KB5029651	N/A
2023-08 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB5029368)	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.	KB5029368	N/A

2023-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5029312)	This cumulative security update includes improvements that are part of update KB5028228 (released July 11, 2023). This update also makes improvements for the following issue: • Kerberos constrained delegation (KCD) might fail with the error message KRB_AP_ERR_MODIFIED on read/write domain controllers after installing the November 2022 security updates. For more information about the resolved security vulnerabilities, please refer to the Deployments I Security Update Guide and the August 2023 Security Updates.	KB5029312	N/A
2023-08 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems (KB5029243)	This security update resolves vulnerabilities in Internet Explorer. To learn more about these vulnerabilities, see Deployments I Security Update Guide.	KB5029243	N/A
2023-08 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems (KB5029243)	This security update resolves vulnerabilities in Internet Explorer. To learn more about these vulnerabilities, see Deployments I Security Update Guide.	KB5029243	N/A
2023-08 Security and Quality Rollup for .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 for x64 (KB5029653)	CVE-2023-36899 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in applications on IIS using their parent application's Application Pool which can lead to privilege escalation or other security bypasses. For more information see CVE 2023-36899. CVE-2023-36873 - .NET Framework Spoofing Vulnerability • This security update addresses a vulnerability where unauthenticated remote attacker can sign ClickOnce deployments without a valid code signing certificate. For more information see CVE-2023-36873.	KB5029653	N/A
2023-08 Security Only Update 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 (KB5029568)	CVE-2023-36899 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in applications on IIS using their parent application's Application Pool which can lead to privilege escalation or other security bypasses. For more information see CVE 2023-36899. CVE-2023-36873 - .NET Framework Spoofing Vulnerability	KB5029568	N/A

	• This security update addresses a vulnerability where unauthenticated remote attacker can sign ClickOnce deployments without a valid code signing certificate. For more information see CVE-2023-36873.		
2023-08 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5029304)	This update makes improvements for the following issue: • Kerberos constrained delegation (KCD) might fail with the error message KRB_AP_ERR_MODIFIED on read/write domain controllers after installing the November 2022 security updates.	KB5029304	N/A
2023-08 Cumulative Update for .NET Framework 4.8 for Windows Server 2016 for x64 (KB5028952)	CVE-2023-36899 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in applications on IIS using their parent application's Application Pool which can lead to privilege escalation or other security bypasses. For more information see CVE 2023-36899. CVE-2023-36873 - .NET Framework Spoofing Vulnerability • This security update addresses a vulnerability where unauthenticated remote attacker can sign ClickOnce deployments without a valid code signing certificate. For more information see CVE-2023-36873.	KB5028952	N/A
2023-08 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB5029247)	This security update includes improvements. When you install this KB: • This update addresses an issue that affects apps that use DirectX on older Intel graphics drivers. You might receive an error from apphelp.dll. • This update affects user mode printer drivers. They unload unexpectedly. This occurs when you print from multiple print queues to the same printer driver. • This update enhances hinting for some of the letters of the Verdana Pro font family. • This update affects the Windows Kernel Vulnerable Driver Blocklist, DriverSiPolicy.p7b. It adds drivers that are at risk for Bring Your Own Vulnerable Driver (BYOVD) attacks. • This update addresses an issue that affects Kerberos constrained delegation (KCD). It fails on read-write domain controllers. The error message is, "KRB_AP_ERR_MODIFIED." This occurs after you install the November 2022 security updates. • This update addresses an issue that affects the Windows Management Instrumentation (WMI) repository. This causes an installation error. The issue occurs when a device does not shut down properly.	KB5029247	N/A

- This update addresses an issue that affects Event Forwarding Subscriptions. When you add an Event Channel to the subscription, it forwards events you do not need.
- This update addresses a deadlock in Internet Protocol Security (IPsec). When you configure servers with IPsec rules, they stop responding. This issue affects virtual and physical servers.
- This update addresses an issue that affects Active Directory Federation Services (AD FS). It might take several attempts to sign in to AD FS successfully. This is because the time calculation for the expiration of a single sign on cookie is wrong.
- This update addresses an issue that affects AD Domains and Trusts snap-ins. They fail to enumerate domain trusts. The error message is, "The parameter is incorrect."

2023-08 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10 Version 1809 for x64 (KB5029647)	CVE-2023-36899 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in applications on IIS using their parent application's Application Pool which can lead to privilege escalation or other security bypasses. For more information see CVE 2023-36899. CVE-2023-36873 - .NET Framework Spoofing Vulnerability • This security update addresses a vulnerability where unauthenticated remote attacker can sign ClickOnce deployments without a valid code signing certificate. For more information see CVE-2023-36873.	KB5029647	N/A
2023-08 Cumulative Update for Windows Server 2019 for x64-based Systems (KB5029247)	This security update includes improvements. When you install this KB: • This update addresses an issue that affects apps that use DirectX on older Intel graphics drivers. You might receive an error from apphelp.dll. • This update affects user mode printer drivers. They unload unexpectedly. This occurs when you print from multiple print queues to the same printer driver. • This update enhances hinting for some of the letters of the Verdana Pro font family. • This update affects the Windows Kernel Vulnerable Driver Blocklist, DriverSiPolicy.p7b. It adds drivers that are at risk for Bring Your Own Vulnerable Driver (BYOVD) attacks. • This update addresses an issue that affects Kerberos constrained delegation (KCD). It fails on read-write domain controllers. The error message is, "KRB_AP_ERR_MODIFIED." This occurs after you install the November 2022 security updates. • This update addresses an issue that affects the Windows Management Instrumentation (WMI) repository. This causes an installation error. The issue occurs when a device does not shut down properly. • This update addresses an issue that affects Event Forwarding Subscriptions. When you add an Event Channel to the subscription, it forwards events you do not need. • This update addresses a deadlock in Internet Protocol Security (IPsec). When you configure servers with IPsec rules, they stop responding. This issue affects virtual and physical servers. • This update addresses an issue that affects Active Directory Federation Services (AD FS). It might take several attempts to sign in to AD FS successfully. This is because the time calculation for the expiration of a single sign on cookie is wrong. • This update addresses an issue that affects AD Domains and Trusts snap-ins. They fail to	KB5029247	N/A

	enumerate domain trusts. The error message is, "The parameter is incorrect."		
2023-08 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 (KB5029647)	CVE-2023-36899 - .NET Framework Remote Code Execution Vulnerability • This security update addresses a vulnerability in applications on IIS using their parent application's Application Pool which can lead to privilege escalation or other security bypasses. For more information see CVE 2023-36899. CVE-2023-36873 - .NET Framework Spoofing Vulnerability • This security update addresses a vulnerability where unauthenticated remote attacker can sign ClickOnce deployments without a valid code signing certificate. For more information see CVE-2023-36873.	KB5029647	N/A
2021-08 Servicing Stack Update for Windows Server 2019 for x64-based Systems (KB5005112)	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.	KB5005112	N/A
Windows Malicious Software Removal Tool x64 - v5.115	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	N/A