BD Product Name: **BD Pyxis™ Supply**

Date of Critical or Security Patches: Jan 2022
Abstract: Critical or Security Patches – Jan 2022

## Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for Jan 2022. 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 |
|---|---|---|---|
| 2022-01 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 KB5008263 (released December 14, 2021) and addresses the following issue:<br>This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release. | KB5009624 | None |
| 2022-01 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 | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. For more information please see CVE-2022-21911. | KB5009721 | None |
| 2022-01 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems | This security update includes quality improvements. Key changes include:<br>This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release. | KB5009595 | None |
| 2022-01 Security Only Update for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, | This security update addresses an issue where an unauthenticated attacker could cause a denial of | KB5009713 | None |

| | | | |
|---|---|---|---|
| 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 for x64 | service on an affected system. For more information please see CVE-2022-21911. | | |
| Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. For more information, see CVE-2022-21911. | KB5008868 | None |
| Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. For more information, see CVE-2022-21911. | KB5008875 | None |
| Security Only Update for .NET Framework 3.5 for Windows 8.1 and Windows Server 2012 R2 | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. For more information, see CVE-2022-21911. | KB5008891 | None |
| Security Only Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 and Windows Server 2012 R2 | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. For more information, see CVE-2022-21911. | KB5008895 | None |
| 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 SP1 and Windows Server 2008 R2 SP1 | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. For more information, see CVE-2022-21911. | KB5009719 | None |
| 2022-01 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems | This security update includes quality improvements. Key changes include:<br>This update contains miscellaneous security improvements to internal OS | KB5009621 | None |

| | | | |
|---|---|---|---|
| | functionality. No specific issues are documented for this release. | | |
| 2022-01 Security Only Update 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 Embedded Standard 7 | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. For more information, see CVE-2022-21911. | KB5009711 | None |
| 2022-01 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 KB5008244 (released December 14, 2021) and addresses the following issues:<br>This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release. | KB5009610 | None |
| Security and Quality Rollup for .NET Framework 4.5.2 for Windows 7 SP1 and Windows Server 2008 R2 SP1 and Windows Server 2008 SP2 | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. For more information, see CVE-2022-21911. | KB5008860 | None |
| Security Only Update for .NET Framework 4.5.2 for Windows 7 SP1 and Windows Server 2008 R2 SP1 and Windows Server 2008 SP2 | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. For more information, see CVE-2022-21911. | KB5008887 | None |
| Security and Quality Rollup for .NET Framework 3.5.1 for Windows 7 SP1 and Windows Server 2008 R2 SP1 | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. For more information, see CVE-2022-21911. | KB5008867 | None |

| | | | |
|---|---|---|---|
| Security Only Update for .NET Framework 3.5.1 for Windows 7 SP1 and Windows Server 2008 R2 SP1 | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. For more information, see CVE-2022-21911. | KB5008890 | None |
| 2022-01 Cumulative Update for Windows Server 2016 for x64-based Systems | This security update includes quality improvements. Key changes include:<br>Addresses an issue that causes searchindexer.exe to stop responding during a dismount operation in the Remote Desktop setup environment.<br>Addresses an issue that causes the BranchCache republication cache to take up more space than it is assigned. This issue occurs if the cache size exceeds 0xFFFFFFFF (4294967295) bytes within a short period (usually within 30 minutes). | KB5009546 | None |
| 2022-01 Cumulative Update for Windows 10 Version 1809 for x86-based Systems | This update contains miscellaneous security improvements to internal OS functionality. No additional issues were documented for this release.Updates security for your Windows operating system. | KB5009557 | None |
| Windows Malicious Software Removal Tool x64 - v5.96 | 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 | None |

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

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

**Microsoft® & Third-Party Patches**

BD has identified patches from Microsoft that have been identified as critical or security related for January 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 | The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers that are running any of the following operating systems:<br>Windows 10<br>Windows Server 2019<br>Windows Server 2016<br>Windows 8.1<br>Windows Server 2012 R2<br>Windows Server 2012<br>Windows Server 2008 R2<br>Windows 7<br>Windows Server 2008<br>OS: Windows Server 2016, Windows Server 2008, Windows Server 2012 | KB890830 | N/A |
| 2022-01 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 KB5008263 (released December 14, 2021) | KB5009624 | NA |
| 2022-01 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 8.1, RT 8.1, and Windows Server 2012 R2 for x64 | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. | KB5009721 | N/A |

| | | | |
|---|---|---|---|
| 2022-01 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems | This security update includes quality improvements. Key changes include:<br>• This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release. | KB5009595 | NA |
| 2022-01 Cumulative Update for Windows Server 2016 for x64-based Systems | This security update includes quality improvements. Key changes include:<br>• Addresses an issue that causes searchindexer.exe to stop responding during a dismount operation in the Remote Desktop setup environment.<br>• Addresses an issue that causes the BranchCache republication cache to take up more space than it is assigned. This issue occurs if the cache size exceeds 0xFFFFFFFF (4294967295) bytes within a short period (usually within 30 minutes). | KB5009546 | NA |

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

Date of Critical or Security Patches: January 2022
Abstract: Critical or Security Patches – January 2022

### Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for January 2022. 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 - v5.97 | The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers that are running any of the following operating systems:<br>Windows 10<br>Windows Server 2019<br>Windows Server 2016<br>Windows 8.1<br>Windows Server 2012 R2<br>Windows Server 2012<br>Windows 7<br>Windows Server 2008 R2 for x64-based Systems | KB890830 | None |
| 2022-01 Cumulative Update for x64-based Systems | This security update includes quality improvements. Key changes include:<br><br>Addresses an issue that causes searchindexer.exe to stop responding during a dismount operation in the Remote Desktop setup environment.<br><br>Addresses an issue that causes the BranchCache republication cache to take up more space than it is assigned. This issue occurs if the cache size exceeds 0xFFFFFFFF (4294967295) bytes within a short period (usually within 30 minutes).Windows 7 | KB5009546 | None |

| | | | |
|---|---|---|---|
| | Windows Server 2008 | | |
| 2022-01 Security Only Update for x64-based Systems | This update contains miscellaneous security improvements to internal OS functionality. | KB5009595 | None |

BD Product Name: **BD Pyxis® PARx**

Date of Critical or Security Patches: Jan 2022
Abstract: Critical or Security Patches – Jan 2022

## Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for Jan 2022. 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 - v5.97 | The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers that are running any of the following operating systems:<br><br>Windows 10<br>Windows Server 2019<br>Windows Server 2016<br>Windows 8.1<br>Windows Server 2012 R2<br>Windows Server 2012<br>Windows Server 2008 R2<br>Windows 7<br>Windows Server 2008 | KB890830 | None |
| 2022-01 Cumulative Update for Windows 10 Version 1607 for x64-based Systems | This security update includes quality improvements. Key changes include:<br><br>Addresses an issue that causes searchindexer.exe to stop responding during a dismount operation in the Remote Desktop setup environment.<br><br>Addresses an issue that causes the BranchCache republication cache to take up more space than | KB5009546 | None |

| | | | |
|---|---|---|---|
| | it is assigned. This issue occurs if the cache size exceeds 0xFFFFFFFF (4294967295) bytes within a short period (usually within 30 minutes).Windows 7 Windows Server 2008 | | |

BD Product Name: **BD Pyxis™ Pharmogistics™**
Date of Critical or Security Patches: January 2022
Abstract: Critical or Security Patches – January 2022

**Microsoft® & Third-Party Patches**

BD has identified patches from Microsoft that have been identified as critical or security related for January 2022. 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:<br>Windows 10<br>Windows Server 2019<br>Windows Server 2016<br>Windows 8.1<br>Windows Server 2012 R2<br>Windows Server 2012<br>Windows 7<br>Windows Server 2008 R2 for x64-based Systems | KB890830 | N/A |
| 2022-01 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems | This security update includes quality improvements. Key changes include:<br>- This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release.<br>For more information about the resolved security vulnerabilities, please refer to the new Security Update Guide website and the January 2022 Security Updates. | KB5009595 | N/A |
| 2022-01 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 KB5008263 (released | KB5009624 | N/A |

| | | | |
|---|---|---|---|
| | December 14, 2021) and addresses the following issue:<br>This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release.<br>For more information about the resolved security vulnerabilities, please refer to the Security Update Guide website and the January 2022 Security Updates. | | |
| 2022-01 Security Only Update 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 | Summary<br>This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. For more information please see CVE-2022-21911. | KB5009713 | N/A |
| 2022-01 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 | Security Improvements<br>This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. For more information please see CVE-2022-21911.<br>Quality Improvements<br>For a list of improvements that were released with this update, please see the article links in the Additional Information section of this article. (See Patch ID link) | KB5009721 | N/A |
| 2022-01 Cumulative Update for Windows 10 Version 20H2 for x64-based Systems | This security update includes quality improvements. Key changes include:<br>Addresses a known issue that affects Japanese Input Method Editors (IME). When you use a Japanese IME to enter text, the text might appear out of order or the text cursor might move unexpectedly in apps that use the multibyte character set (MBCS). This issue affects the Microsoft Japanese IME and third-party Japanese IMEs. | KB5009543 | N/A |

| | | | |
|---|---|---|---|
| 2022-01 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 20H2 for x64 | Security Improvements<br>This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. For more information please see CVE-2022-21911.<br>Quality and reliability improvements<br>WPF1<br>- Addresses an issue where WPF does not respond to touch if the WPF window was activated by a touch manipulation (e.g. swiping a listbox).<br>- Adds a mitigation for an issue involving tearing, flickering, or incorrect composition of visual content under high GPU-load conditions. | KB5008876 | N/A |
| 2022-01 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 Server 2008 R2 for x64 | Security Improvements<br>This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. For more information please see CVE-2022-21911.<br>Quality Improvements<br>For a list of improvements that were released with this update, please see the article links in the Additional Information section of this article. | KB5009719 | N/A |
| 2022-01 Security Only Update 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 Server 2008 R2 for x64 | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. For more information please see CVE-2022-21911. | KB5009711 | N/A |

| | | | |
|---|---|---|---|
| 2022-01 Security Only Quality Update for Windows Server 2008 R2 for x64-based Systems | Improvements and fixes<br>This security update includes quality improvements. Key changes include:<br>This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release. | KB5009621 | N/A |
| 2022-01 Cumulative Update for Windows Server 2016 for x64-based Systems | Improvements and fixes<br>This security update includes quality improvements. Key changes include:<br>Addresses an issue that causes searchindexer.exe to stop responding during a dismount operation in the Remote Desktop setup environment.<br>Addresses an issue that causes the BranchCache republication cache to take up more space than it is assigned. This issue occurs if the cache size exceeds 0xFFFFFFFF (4294967295) bytes within a short period (usually within 30 minutes). | KB5009546 | N/A |

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

Date of Critical or Security Patches - January 2022
Abstract: Critical or Security Patches - January 2022

**Microsoft® & Third-Party Patches**

BD has identified patches from Microsoft that have been identified as critical or security related for January 2022. 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 - v5.97 | The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers. | KB890830 | N/A |
| 2022-01 Cumulative Update for Windows 10 Version 1607 for x64-based Systems. | This security update includes quality improvements. Key changes include:<br>Addresses an issue that causes searchindexer.exe to stop responding during a dismount operation in the Remote Desktop setup environment.<br>Addresses an issue that causes the BranchCache republication cache to take up more space than it is assigned. This issue occurs if the cache size exceeds 0xFFFFFFFF (4294967295) bytes within a short period (usually within 30 minutes). | KB5009546 | N/A |
| 2022-01 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 KB5008244 (released December 14, 2021) and addresses the following issues:<br>This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release. | KB5009610 | N/A |

| | | | |
|---|---|---|---|
| 2022-01 Security Only Update 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 Embedded Standard 7. | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. | KB5009711 | N/A |
| 2022-01 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems. | This security update includes quality improvements. Key changes include:<br>This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release. | KB5009621 | N/A |
| 2022-01 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 Embedded Standard 7. | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. | KB5009719 | N/A |

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

Date of Critical or Security Patches - January 2022
Abstract: Critical or Security Patches - January 2022

### Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for January 2022. 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 |
|---|---|---|---|
| 2022-01 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 KB5008244 (released December 14, 2021) and addresses the following issues:<br>This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release. | KB5009610 | N/A |
| 2022-01 Security Only Update 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 Embedded Standard 7. | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. | KB5009711 | N/A |
| 2022-01 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems. | This security update includes quality improvements. Key changes include:<br>This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release. | KB5009621 | N/A |

|  |  |  |  |
|---|---|---|---|
| 2022-01 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 Embedded Standard 7. | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. | KB5009719 | N/A |

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

Date of Critical or Security Patches - January 2022
Abstract: Critical or Security Patches - January 2022

**Microsoft® & Third-Party Patches**

BD has identified patches from Microsoft that have been identified as critical or security related for January 2022. 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 - v5.97 | The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers. | KB890830 | N/A |
| 2022-01 Security and Quality Rollup for .NET Framework 2.0, 3.0, 4.5.2, 4.6 and 4.6.2 for Windows Server 2008 SP2. | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. | KB5009722 | N/A |
| 2022-01 Security Only Quality Update for Windows Server 2008 for x86-based Systems. | This security update includes quality improvements. Key changes include: This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release. | KB5009601 | N/A |
| 2022-01 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 KB5008274 (released December 14, 2021) and addresses the following issue:<br>This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release. | KB5009627 | N/A |
| 2022-01 Security Only Update for .NET Framework 2.0, 3.0, 4.5.2, 4.6 and 4.6.2 for Windows Server 2008 SP2. | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. | KB5009714 | N/A |

| | | | |
|---|---|---|---|
| 2022-01 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 KB5008244 (released December 14, 2021) and addresses the following issues:<br>This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release. | KB5009610 | N/A |
| 2022-01 Security Only Update 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 Embedded Standard 7. | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. | KB5009711 | N/A |
| 2022-01 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems. | This security update includes quality improvements. Key changes include:<br>This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release. | KB5009621 | N/A |
| 2022-01 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 Embedded Standard 7. | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. | KB5009719 | N/A |

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

Date of Critical or Security Patches - January 2022
Abstract: Critical or Security Patches – January 2022

## Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for January 2022. 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 - v5.97 | The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers. | KB890830 | N/A |
| 2022-01 Cumulative Update for Windows Server 2016 for x64-based Systems. | This security update includes quality improvements. Key changes include:<br>Addresses an issue that causes searchindexer.exe to stop responding during a dismount operation in the Remote Desktop setup environment.<br>Addresses an issue that causes the BranchCache republication cache to take up more space than it is assigned. This issue occurs if the cache size exceeds 0xFFFFFFFF (4294967295) bytes within a short period (usually within 30 minutes). | KB5009546 | N/A |
| 2022-01 Cumulative Update for Windows 10 Version 1607 for x64-based Systems. | This security update includes quality improvements. Key changes include:<br>Addresses an issue that causes searchindexer.exe to stop responding during a dismount operation in the Remote Desktop setup environment.<br>Addresses an issue that causes the BranchCache republication cache to take up more space than it is assigned. This issue occurs if the cache size exceeds | KB5009546 | N/A |

| | | | |
|---|---|---|---|
| | 0xFFFFFFFF (4294967295) bytes within a short period (usually within 30 minutes). | | |
| 2022-01 Cumulative Update for Windows 10 Version 1607 for x64-based Systems. | This non-security update includes quality improvements. Key changes include:<br>Addresses a known issue that might cause IP Security (IPSEC) connections that contain a Vendor ID to fail. VPN connections using Layer 2 Tunneling Protocol (L2TP) or IP security Internet Key Exchange (IPSEC IKE) might also be affected.<br>Addresses a known issue that might cause Windows Servers to restart unexpectedly after installing the January 11, 2022 update on domain controllers (DCs).<br>Addresses an issue that prevents Active Directory (AD) attributes from being written properly during a Lightweight Directory Access Protocol (LDAP) modify operation when you make multiple attribute changes.<br>Addresses an issue that might prevent removable media that is formatted using the Resilient File System (ReFS) from mounting or might cause the removable media to mount in the RAW file format. This issue occurs after installing the January 11, 2022 Windows update. | KB5010790 | N/A |
| Windows Malicious Software Removal Tool - v5.97 | The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers. | KB890830 | N/A |
| 2022-01 Security and QualityRollup for .NET Framework 2.0, 3.0, 4.5.2, 4.6 and 4.6.2 for Windows Server 2008 SP2. | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. | KB5009722 | N/A |

| | | | |
|---|---|---|---|
| 2022-01Security Only Quality Update for Windows Server 2008 for x86-based Systems. | This security update includes quality improvements. Key changes include:<br>This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release. | KB5009601 | N/A |
| 2022-01Security MonthlyQuality Rollup for Windows Server 2008 for x86-based Systems. | This security update includes improvements and fixes that were a part of update KB5008274 (released December 14, 2021) and addresses the following issue:<br>This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release. | KB5009627 | N/A |
| 2022-01Security Only Update for .NET Framework 2.0, 3.0, 4.5.2, 4.6 and 4.6.2 for Windows Server 2008 SP2. | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. | KB5009714 | N/A |
| 2022-01 Security MonthlyQuality Rollup forWindows Embedded Standard 7 for x86-based Systems. | This security update includes improvements and fixes that were a part of update KB5008244 (released December 14, 2021) and addresses the following issues:<br>This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release. | KB5009610 | N/A |
| 2022-01 Security Only Update 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 Embedded Standard 7. | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. | KB5009711 | N/A |

| | | | |
|---|---|---|---|
| 2022-01 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems. | This security update includes quality improvements. Key changes include:<br>This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release. | KB5009621 | N/A |
| 2022-01 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 Embedded Standard 7. | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. | KB5009719 | N/A |

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

Date of Critical or Security Patches: January 2022
Abstract: Critical or Security Patches – January 2022

**Microsoft® & Third-Party Patches**

BD has identified patches from Microsoft that have been identified as critical or security related for January 2022. 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 |
|---|---|---|---|
| 2022-01 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 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. | KB 5009719 | N/A |
| 2021-10 Security Monthly Quality Rollup for Windows 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. | KB5006743 | N/A |

| | | | |
|---|---|---|---|
| https://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=8e39f2d7-a4de-4567-a305-61aaab5ee92b | 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. | KB5006749 | N/A |
| 2022-01 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x64-based Systems | A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system. | KB5009610 | N/A |
| 2022-01 Update for Windows Server 2008 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. | KB5010798 | N/A |

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

Date of Critical or Security Patches: January 2022
Abstract: Critical or Security Patches – January 2022

### Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for January 2022. 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 |
|---|---|---|---|
| 2022-01 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. | KB5009624 | 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 |

|  |  |  |  |
|---|---|---|---|
| 2022-01 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 | 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 | KB5009721 | None |
| 2022-01 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. | KB5009595 | None |
| 2022-01 Security Only Update 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 | 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. | KB5009713 | None |
| 2022-01 Security and Quality Rollup for .NET Framework 3.5 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. | KB5008868 | None |

| | | | |
|---|---|---|---|
| 2022-01 Security and Quality Rollup for .NET Framework 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. | KB5008883 | None |
| 2022-01 Security Only Update for .NET Framework 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. | KB5008897 | None |
| 2022-01 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. | KB5009546 | None |
| 2022-01 Security Only Update for .NET Framework 3.5 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. | KB5008891 | None |

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

Date of Critical or Security Patches: January 2022

Abstract: Critical or Security Patches – January 2022

**Microsoft® & Third-Party Patches**

BD has identified patches from Microsoft that have been identified as critical or security related for January 2022. 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 maintain the correct security posture of the system(s).

| Patch Name | Description | Patch ID | Notes |
|---|---|---|---|
| 2022-01 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 KB5008244 (released December 14, 2021) and addresses the following issues:<br>This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release. | KB5009610 | N/A |
| 2022-01 Security Only Update 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 Embedded Standard 7 | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. For more information, see CVE-2022-21911. | KB5009711 | N/A |

|  |  |  |  |
|---|---|---|---|
| 2022-01 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems | This security update includes quality improvements. Key changes include:<br>This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release. | KB5009621 | N/A |
| 2022-01 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 Embedded Standard 7. | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. | KB5009719 | N/A |
| 2022-01 Cumulative Update for Windows 10 Version 1607 for x64-based Systems | This security update includes quality improvements. Key changes include:<br>Addresses an issue that causes searchindexer.exe to stop responding during a dismount operation in the Remote Desktop setup environment.<br>Addresses an issue that causes the BranchCache republication cache to take up more space than it is assigned. This issue occurs if the cache size exceeds 0xFFFFFFFF (4294967295) bytes within a short period (usually within 30 minutes).Windows 7<br>Windows Server 2008 | KB5009546 | N/A |
| Windows Malicious Software Removal Tool x64 - v5.97 | The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers that are running any of the following operating systems: | KB890830 | N/A |

| | | | |
|---|---|---|---|
| | Windows 10<br>Windows Server 2019<br>Windows Server 2016<br>Windows 8.1<br>Windows Server 2012 R2<br>Windows Server 2012<br>Windows Server 2008 R2<br>Windows 7<br>Windows Server 2008 | | |
| 2022-01 Cumulative Update for Windows 10 Version 1809 for x86-based Systems | This update contains miscellaneous security improvements to internal OS functionality. No additional issues were documented for this release.Updates security for your Windows operating system. | KB5009557 | N/A |
| 2022-01 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. | KB5009718 | N/A |
| 2022-01 Cumulative Update for Windows 10 Version 1809 for x64-based Systems | A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system. | **KB5009557** | N/A |
| 2022-01 Cumulative Update for Windows | This non-security update includes quality | KB5010790 | N/A |

| | | | |
|---|---|---|---|
| 10 Version 1607 for x64-based Systems. | improvements. Key changes include:<br>Addresses a known issue that might cause IP Security (IPSEC) connections that contain a Vendor ID to fail. VPN connections using Layer 2 Tunneling Protocol (L2TP) or IP security Internet Key Exchange (IPSEC IKE) might also be affected.<br>Addresses a known issue that might cause Windows Servers to restart unexpectedly after installing the January 11, 2022 update on domain controllers (DCs).<br>Addresses an issue that prevents Active Directory (AD) attributes from being written properly during a Lightweight Directory Access Protocol (LDAP) modify operation when you make multiple attribute changes.<br>Addresses an issue that might prevent removable media that is formatted using the Resilient File System (ReFS) from mounting or might cause the removable media to mount in the RAW file format. This issue occurs after installing the January 11, 2022 Windows update. | | |

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

Date of Critical or Security Patches: January 2022

Abstract: Critical or Security Patches – January 2022

### Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for January 2022. 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 |
|---|---|---|---|
| 2022-01 Security Only Update 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 | 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. | KB5009713 | N/A |
| 2022-01 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 KB5008263 (released December 14, 2021) and addresses the following issue:<br>This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release. | KB5009624 | N/A |

| | | | |
|---|---|---|---|
| 2022-01 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems | This security update includes quality improvements. Key changes include:<br>This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release. | KB5009595 | N/A |
| 2022-01 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 | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. For more information please see CVE-2022-21911. | KB5009721 | N/A |
| Windows Malicious Software Removal Tool x64 - v5.97 | The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers that are running any of the following operating systems:<br><br>Windows 10<br>Windows Server 2019<br>Windows Server 2016<br>Windows 8.1<br>Windows Server 2012 R2<br>Windows Server 2012<br>Windows Server 2008 R2<br>Windows 7<br>Windows Server 2008 | KB890830 | N/A |
| 2022-01 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 Embedded Standard 7. | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. | KB5009719 | N/A |
| 2022-01 Security Monthly Quality Rollup for Windows Embedded Standard | This security update includes improvements and fixes that were a part of update KB5008244 (released December 14, 2021) and | KB5009610 | N/A |

| | | | |
|---|---|---|---|
| 7 for x86-based Systems | addresses the following issues:<br>This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release. | | |
| 2022-01 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems | This security update includes quality improvements. Key changes include:<br>This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release. | KB5009621 | N/A |
| 2022-01 Security Only Update 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 Embedded Standard 7 | This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system. For more information, see CVE-2022-21911. | KB5009711 | N/A |
| 2022-01 Cumulative Update for Windows 10 Version 1607 for x64-based Systems. | This non-security update includes quality improvements. Key changes include:<br>Addresses a known issue that might cause IP Security (IPSEC) connections that contain a Vendor ID to fail. VPN connections using Layer 2 Tunneling Protocol (L2TP) or IP security Internet Key Exchange (IPSEC IKE) might also be affected.<br>Addresses a known issue that might cause Windows Servers to restart unexpectedly after installing the January 11, 2022 update on domain controllers (DCs).<br>Addresses an issue that prevents Active Directory (AD) attributes from being written properly during a Lightweight Directory Access | KB5010790 | N/A |

|  |  |  |  |
|---|---|---|---|
|  | Protocol (LDAP) modify operation when you make multiple attribute changes.<br>Addresses an issue that might prevent removable media that is formatted using the Resilient File System (ReFS) from mounting or might cause the removable media to mount in the RAW file format. This issue occurs after installing the January 11, 2022 Windows update. |  |  |
| 2022-01 Cumulative Update for Windows Server 2016 for x64-based Systems | This security update includes quality improvements. Key changes include:<br>Addresses an issue that causes searchindexer.exe to stop responding during a dismount operation in the Remote Desktop setup environment.<br>Addresses an issue that causes the BranchCache republication cache to take up more space than it is assigned. This issue occurs if the cache size exceeds 0xFFFFFFFF (4294967295) bytes within a short period (usually within 30 minutes). | KB5009546 | N/A |
| 2022-01 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.<br>After you install this update, you may have to restart your system. | KB5009718 | N/A |
| 2022-01 Cumulative Update for Windows 10 Version 1809 for x64-based Systems | A security issue has been identified in a Microsoft software product that could affect your system. You can | KB5009557 | N/A |

| | | | |
|---|---|---|---|
| | 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.<br>After you install this update, you may have to restart your system. | | |
| 2022-01 Cumulative Update for Windows 10 Version 1607 for x64-based Systems | This security update includes quality improvements. Key changes include:<br>Addresses an issue that causes searchindexer.exe to stop responding during a dismount operation in the Remote Desktop setup environment.<br>Addresses an issue that causes the BranchCache republication cache to take up more space than it is assigned. This issue occurs if the cache size exceeds 0xFFFFFFFF (4294967295) bytes within a short period (usually within 30 minutes).Windows 7<br>Windows Server 2008 | KB5009546 | N/A |