

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

Date of Critical or Security Patches: March 2021

Abstract: Critical or Security Patches – March 2021

### Microsoft® & Third-Party Patches

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

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

Patch Name	Description	Patch ID	Notes
2021-03 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,	<a href="#">KB5000803</a>	None
2021-01 Update for Windows Server 2016 for x64-based Systems	Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information.	<a href="#">KB4589210</a>	None
Windows Malicious Software Removal Tool x64 - v5.87	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	<a href="#">KB890830</a>	None



2021-03 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	<a href="#">KB5000848</a>	None
--	---	---------------------------	------

BD Product Name: **BD Pyxis™ CII Safe ES**

Date of Critical or Security Patches: March 2021

Abstract: Critical or Security Patches – March 2021

### Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for March 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
Security Update for Microsoft windows	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.	<a href="#">KB5000859</a>	None
2021-03 Cumulative Update for Windows 10	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.	<a href="#">KB5000822</a>	None



BD Product Name: **BD Pyxis® PARx**

Date of Critical or Security Patches: March 2021

Abstract: Critical or Security Patches – March 2021

### **Microsoft® & Third-Party Patches**

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

<b>Patch Name</b>	<b>Description</b>	<b>Patch ID</b>	<b>Notes</b>
Malicious Software Removal Tool - KB890830 (Version 5.86)	Microsoft Patch KB890830 is a "Malicious Software Removal Tool" that was released to provide an immediate solution for computers infected with the Blaster, Sasser and MyDoom viruses	<a href="#">KB890830</a>	N/A

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

Date of Critical or Security Patches: March 2021

Abstract: Critical or Security Patches – March 2021

### Microsoft® & Third-Party Patches

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

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

Patch Name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.86	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers that are running any of the following operating systems: Windows 10 Windows Server 2019 Windows Server 2016 Windows 8.1 Windows Server 2012 R2 Windows Server 2012 Windows 7 Windows Server 2008 R2 for x64-based Systems	<a href="#">KB890830</a>	N/A
Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems	This security update will update Internet Explorer to version 11.	<a href="#">KB5000800</a>	N/A
2021-03 Security Only Quality Update for Windows Server 2012 R2	This security update is a cumulative monthly security updates as Windows Server 2012 R2 have reached the end of mainstream support and are now in extended support. This security update includes quality improvements. Key changes:	<a href="#">KB5000853</a>	N/A



	<ul style="list-style-type: none"> <li>Addresses an issue in which a non-native device that is in the same realm does not receive a Kerberos Service ticket from Active Directory DCs.</li> <li>Security updates to Windows Fundamentals, Windows Shell, Windows UAC, Windows Hybrid Cloud Networking, Windows Media, and Windows Graphics.</li> </ul>		
2021-03 Security Monthly Quality Rollup for Windows Server 2012 R2	This security update includes improvements and fixes that were a part of update KB4601384 (released February 9, 2021).	<a href="#">KB5000848</a>	N/A

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

Date of Critical or Security Patches: March 2021

Abstract: Critical or Security Patches – March 2021

### Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for March 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 - v5.87	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	<a href="#">KB890830</a>	N/A
2021-03 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This security update includes quality improvements. Key changes include:  Addresses an issue in which a non-native device that is in the same realm does not receive a Kerberos Service ticket from Active Directory DCs. This issue occurs even though Windows Updates are installed that contain CVE-2020-17049 protections released between November 10 and December 8, 2020 and configured PerfromTicketSignature to 1 or larger. Ticket acquisition fails with KRB_GENERIC_ERROR if callers submit a PAC-less Ticket Granting Ticket (TGT) as an evidence ticket without the	<a href="#">KB5000851</a>	N/A



	<p>USER_NO_AUTH_DATA_REQ UIRED flag being set for the user in User Account Controls.</p> <p>Security updates to Windows Fundamentals, Windows Shell, Windows UAC, Windows Hybrid Cloud Networking, and Windows Media.</p>		
2021-03 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	<p>Turns off token binding by default in Windows Internet (WinINet).</p> <p>Addresses an issue in the Windows Management Instrumentation (WMI) service that causes a heap leak each time security settings are applied to WMI namespace permissions.</p> <p>Addresses a reliability issue in Remote Desktop.</p> <p>Addresses an issue that might cause stop error 7E in nfssvr.sys on servers running the Network File System (NFS) service.</p>	<a href="#">KB5000803</a>	N/A
Update for Removal of Adobe Flash Player for Windows 10 Version 1607 for x86-based systems	This update removes Adobe Flash Player that is installed on any of the Windows operating systems that are listed in the "Applies to" section. After you apply this update, it cannot be uninstalled.	<a href="#">KB4577586</a>	N/A
2021-03 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems	This security update resolves vulnerabilities in Internet Explorer. To learn more about these vulnerabilities, see Microsoft Common Vulnerabilities and Exposures.	<a href="#">KB5000800</a>	N/A



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

Date of Critical or Security Patches: March 2021

Abstract: Critical or Security Patches – March 2021

### Microsoft® & Third-Party Patches

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

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

Patch Name	Description	Patch ID	Notes
2021-03 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems	This security update resolves vulnerabilities in Internet Explorer. To learn more about these vulnerabilities, see Microsoft Common Vulnerabilities and Exposures.	<a href="#">KB5000800</a>	N/A
2021-03 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This security update includes quality improvements. Key changes include:  Addresses an issue in which a non-native device that is in the same realm does not receive a Kerberos Service ticket from Active Directory DCs. This issue occurs even though Windows Updates are installed that contain CVE-2020-17049 protections released between November 10 and December 8, 2020 and configured PerfromTicketSignature to 1 or larger. Ticket acquisition fails with KRB_GENERIC_ERROR if callers submit a PAC-less Ticket Granting Ticket (TGT) as an evidence ticket without the	<a href="#">KB5000851</a>	N/A



	<p>USER_NO_AUTH_DATA_REQUIRED flag being set for the user in User Account Controls.</p> <p>Security updates to Windows Fundamentals, Windows Shell, Windows UAC, Windows Hybrid Cloud Networking, and Windows Media.</p>		
--	--	--	--

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

Date of Critical or Security Patches: March 2021

Abstract: Critical or Security Patches – March 2021

### Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for March 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 - v5.87	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	<a href="#">KB890830</a>	N/A
2021-03 Cumulative Security Update for Internet Explorer 11 for Windows Embedded Standard 7 for x86-based systems	This security update resolves vulnerabilities in Internet Explorer. To learn more about these vulnerabilities, see Microsoft Common Vulnerabilities and Exposures.	<a href="#">KB5000800</a>	N/A
2021-03 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	This security update includes quality improvements. Key changes include:  Addresses an issue in which a non-native device that is in the same realm does not receive a Kerberos Service ticket from Active Directory DCs. This issue occurs even though Windows Updates are installed that contain CVE-2020-17049 protections released between November 10 and December 8, 2020 and configured	<a href="#">KB5000851</a>	N/A



	<p>PerfromTicketSignature to 1 or larger. Ticket acquisition fails with KRB_GENERIC_ERROR if callers submit a PAC-less Ticket Granting Ticket (TGT) as an evidence ticket without the USER_NO_AUTH_DATA_REQUIRED flag being set for the user in User Account Controls.</p> <p>Security updates to Windows Fundamentals, Windows Shell, Windows UAC, Windows Hybrid Cloud Networking, and Windows Media.</p>		
--	---	--	--

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

Date of Critical or Security Patches: March 2021

Abstract: Critical or Security Patches – March 2021

### Microsoft® & Third-Party Patches

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

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

Patch Name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.87	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	<a href="#">KB890830</a>	N/A
2021-03 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	<p>This security update includes quality improvements. Key changes include:</p> <ul style="list-style-type: none"><li>Turns off token binding by default in Windows Internet (WinINet).</li><li>Addresses an issue in the Windows Management Instrumentation (WMI) service that causes a heap leak each time security settings are applied to WMI namespace permissions.</li><li>Addresses a reliability issue in Remote Desktop.</li><li>Addresses an issue that might cause stop error 7E in nfssvr.sys on servers running the Network File System (NFS) service.</li></ul>	<a href="#">KB5000803</a>	N/A



Windows Malicious Software Removal Tool - v5.87	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	<a href="#">KB890830</a>	N/A
2021-03 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems	<p>This security update includes quality improvements. Key changes include:</p> <p>Addresses an issue in which a non-native device that is in the same realm does not receive a Kerberos Service ticket from Active Directory DCs. This issue occurs even though Windows Updates are installed that contain CVE-2020-17049 protections released between November 10 and December 8, 2020 and configured PerfromTicketSignature to 1 or larger. Ticket acquisition fails with KRB_GENERIC_ERROR if callers submit a PAC-less Ticket Granting Ticket (TGT) as an evidence ticket without the USER_NO_AUTH_DATA_REQUIRED flag being set for the user in User Account Controls.</p> <p>Security updates to Windows Fundamentals, Windows Shell, Windows UAC, Windows Hybrid Cloud Networking, and Windows Media.</p>	<a href="#">KB5000851</a>	N/A
Update for Removal of Adobe Flash Player for Windows 10 Version 1607 for x64-based systems	This update removes Adobe Flash Player that is installed on any of the Windows operating systems that are listed in the "Applies to" section. After you apply this update, it cannot be uninstalled.	<a href="#">KB4577586</a>	N/A

BD Product Name: **BD Pyxis™ Supply**

Date of Critical or Security Patches: March 2021

Abstract: Critical or Security Patches – March 2021

### **Microsoft® & Third-Party Patches**

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

<b>Patch Name</b>	<b>Description</b>	<b>Patch ID</b>	<b>Notes</b>
2021-03 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems	<p>This security update resolves vulnerabilities in Internet Explorer.</p> <p>The fixes that are included in this update are also included in the March 2021 Security Monthly Quality Rollup. Installing either this update or the Security Monthly Quality Rollup installs the same fixes.</p> <p>This update is not applicable for installation on a device on which the Security Monthly Quality Rollup or the Preview of Monthly Quality Rollup from March 2021 (or a later month) is already installed. This is because those updates contain all the same fixes that are included in this update.</p> <p>If you use update management processes other than Windows Update and you automatically approve all security update classifications for deployment, this update, the March 2021 Security Only</p>	<a href="#">KB5000800</a>	None



	<p>Quality Update, and the March 2021 Security Monthly Quality Rollup are deployed. We recommend that you review your update deployment rules to make sure that the desired updates are deployed.</p> <p>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 <a href="#">Add language packs to Windows</a>.</p>		
<p>2021-03 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems</p>	<p>This security update includes improvements and fixes that were a part of update KB4601384 (released February 9, 2021) and addresses the following issues:</p> <p>Addresses an issue in which a non-native device that is in the same realm does not receive a Kerberos Service ticket from Active Directory DCs. This issue occurs even though Windows Updates are installed that contain CVE-2020-17049 protections released between November 10 and December 8, 2020 and configured PerfromTicketSignature to 1 or larger. Ticket acquisition fails with KRB_GENERIC_ERROR if callers submit a PAC-less Ticket Granting Ticket (TGT) as an evidence ticket without the USER_NO_AUTH_DATA_REQ UIRED flag being set for the</p>	<p><a href="#">KB5000848</a></p>	<p>None</p>



	<p>user in User Account Controls.</p> <p>Addresses an elevation of privilege security vulnerability documented in CVE-2021-1640 related to print jobs submitted to "FILE:" ports. After installing Windows updates from March 9, 2021 and later, print jobs that are in a pending state before restarting the print spooler service or restarting the OS will remain in an error state. Manually delete the affected print jobs and resubmit them to the print queue when the print spooler service is online.</p> <p>Security updates to Windows Fundamentals, Windows Shell, Windows UAC, Windows Hybrid Cloud Networking, Windows Media, and Windows Graphics.</p>		
<p>2021-03 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems</p>	<p>This security update includes quality improvements. Key changes include:</p> <p>Addresses an issue in which a non-native device that is in the same realm does not receive a Kerberos Service ticket from Active Directory DCs. This issue occurs even though Windows Updates are installed that contain CVE-2020-17049 protections released between November 10 and December 8, 2020 and configured PerfromTicketSignature to 1 or larger. Ticket acquisition fails with KRB_GENERIC_ERROR if callers submit a PAC-less Ticket Granting Ticket (TGT) as an evidence ticket without the</p>	<p><a href="#">KB5000853</a></p>	<p>None</p>

	<p>USER_NO_AUTH_DATA_REQUIRED flag being set for the user in User Account Controls.</p> <p>Security updates to Windows Fundamentals, Windows Shell, Windows UAC, Windows Hybrid Cloud Networking, Windows Media, and Windows Graphics.</p>		
<p>2021-03 Security Only Quality Update for Windows Embedded Standard 7 for x64-based Systems</p>	<p>This security update includes quality improvements. Key changes include:</p> <p>Addresses an issue in which a non-native device that is in the same realm does not receive a Kerberos Service ticket from Active Directory DCs. This issue occurs even though Windows Updates are installed that contain CVE-2020-17049 protections released between November 10 and December 8, 2020 and configured PerfromTicketSignature to 1 or larger. Ticket acquisition fails with KRB_GENERIC_ERROR if callers submit a PAC-less Ticket Granting Ticket (TGT) as an evidence ticket without the USER_NO_AUTH_DATA_REQUIRED flag being set for the user in User Account Controls.</p> <p>Security updates to Windows Fundamentals, Windows Shell, Windows UAC, Windows Hybrid Cloud Networking, and Windows Media.</p>	<p><a href="#">KB5000851</a></p>	<p>None</p>

<p>2021-03 Cumulative Update for Windows 10 Version 1607 for x64-based Systems</p>	<p>Updates security for the Windows user interface.</p> <p>Updates to improve security when Windows performs basic operations.</p> <p>Updates to improve security when using Microsoft Office products.</p>	<p><a href="#">KB5000803</a></p>	<p>None</p>
<p>2021-01 Update for Windows Server 2016 for x64-based Systems</p>	<p>This update is a standalone update that is targeted at Windows 10, version 1607 and Windows Server 2016. This update also includes Intel microcode updates that were already released for these operating systems at the time of release. We will offer additional microcode updates from Intel through this article for these operating systems as they become available to Microsoft. Use the registry settings as described in the Windows client and Windows Server KB articles.</p>	<p><a href="#">KB4589210</a></p>	<p>None</p>
<p>2021-03 Servicing Stack Update for Windows 10 Version 1809 for x64-based Systems</p>	<p>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.</p> <p>This update applies to the following:</p>	<p><a href="#">KB5000859</a></p>	<p>None</p>

	<p>Windows 10, version 1809 for 32-bit systems.</p> <p>Windows 10, version 1809 for ARM64-based systems.</p> <p>Windows 10, version 1809 for x64-based systems.</p> <p>Windows Server 2019.</p> <p>Windows Server 2019 (Server Core installation).</p>		
<p>2021-03 Cumulative Update for Windows 10 Version 1809 for x64-based Systems</p>	<p>This security update Addresses an elevation of privilege security vulnerability documented in CVE-2021-1640 related to print jobs submitted to "FILE:" ports. After installing Windows updates from March 9, 2021 and later, print jobs that are in a pending state before restarting the print spooler service or restarting the OS will remain in an error state. Manually delete the affected print jobs and resubmit them to the print queue when the print spooler service is online.</p> <p>Security updates to the Windows Shell, Windows Fundamentals, Windows Management, Windows Apps, Windows User Account Control (UAC), Windows Core Networking, Windows Hybrid Cloud Networking, the Windows Kernel, Windows Virtualization, the Microsoft Graphics Component, Internet Explorer, Microsoft Edge Legacy, and Windows Media.</p>	<p><a href="#">KB5000822</a></p>	<p>None</p>
<p>2021-01 Update for Windows 10 Version 1809 for x64-based Systems</p>	<p>This update is a standalone update that is targeted at Windows 10, version 1809 and Windows Server 2019. This update also includes Intel microcode updates that were already released for these operating systems at</p>	<p><a href="#">KB4589208</a></p>	<p>None</p>

	<p>the time of release. We will offer additional microcode updates from Intel through this article for these operating systems as they become available to Microsoft. Use the registry settings as described in the Windows client and Windows Server KB articles.</p>		
<p>2021-03 Cumulative Update for Windows 10 Version 2004 for x64-based Systems</p>	<p>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.</p> <p>This update applies to the following:</p> <p>Windows 10 Version 1607 for 32-bit Systems</p> <p>Windows 10 Version 1607 for x64-based Systems</p> <p>Windows Server 2016</p> <p>Windows Server 2016 (Server Core installation)</p>	<p><a href="#">KB5000802</a></p>	<p>None</p>
<p>Update for Removal of Adobe Flash Player for Windows 10 Version 1803 for x64-based systems</p>	<p>This update removes Adobe Flash Player that is installed on any of the Windows operating systems that are listed in the "Applies to" section. After you apply this update, it cannot be uninstalled.</p>	<p><a href="#">KB4577586</a></p>	<p>None</p>
<p>Cumulative Update Preview for .NET Framework 3.5 and 4.8 for Windows 10, version 2004, Windows Server, version 2004, Windows 10, version 20H2, and</p>	<p>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</p>	<p><a href="#">KB4601554</a></p>	<p>None</p>

<p>Windows Server, version 20H2</p>	<p>so that your devices can receive and install Microsoft updates. Additionally, this update enables a single package design that incorporates the servicing stack update (SSU) into the latest cumulative update (LCU). Combining the SSU and LCU update into a single package provides a more seamless deployment and installation experience.</p> <p>This update applies to the following:</p> <p>Windows 10 Version 1809 for 32-bit Systems</p> <p>Windows 10 Version 1809 for ARM64-based Systems</p> <p>Windows 10 Version 1809 for x64-based Systems</p> <p>Windows Server 2019</p> <p>Windows Server 2019 (Server Core installation)</p>		
<p>2021-01 Update for Windows 10 Version 2004 for x64-based Systems</p>	<p>We recommend that you reinstall this update to make sure you have the latest updates. This update is a standalone update that is targeted at Windows 10, version 2004 and 20H2, and Windows Server, version 2004 and 20H2. This update also includes Intel microcode updates that were already released for these operating systems at the time of release. We will offer additional microcode updates from Intel through this article for these operating systems as they become available to Microsoft. Use the registry</p>	<p><a href="#">KB4589212</a></p>	<p>None</p>

	settings as described in the Windows client and Windows Server KB articles. (By default, these registry settings are enabled for Windows client OS editions and Windows Server OS editions.)		
Security intelligence updates for Microsoft Defender Antivirus and other Microsoft antimalware	Microsoft continually updates security intelligence in antimalware products to cover the latest threats and to constantly tweak detection logic, enhancing the ability of Microsoft Defender Antivirus and other Microsoft antimalware solutions to accurately identify threats. This security intelligence works directly with cloud-based protection to deliver fast and powerful AI-enhanced, next-generation protection.	<a href="#">KB2267602</a>	None
Remove specific prevalent malware with 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:  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	<a href="#">KB890830</a>	None

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

Date of Critical or Security Patches: March 2021

Abstract: Critical or Security Patches – March 2021

### Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for March 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
Security Update for Microsoft Excel 2013 32-Bit Edition	A security vulnerability exists in Microsoft Excel 2013 32-Bit Edition that could allow arbitrary code to run when a maliciously modified file is opened. This update resolves that vulnerability.	<a href="#">KB4493239</a>	N/A
Security Update for Microsoft Office 2013 64-Bit Edition	A security vulnerability exists in Microsoft Office 2013 64-Bit Edition that could allow arbitrary code to run when a maliciously modified file is opened. This update resolves that vulnerability.	<a href="#">KB4493228</a>	N/A
Security Update for Microsoft Office 2013 64-Bit Edition	A security vulnerability exists in Microsoft Office 2013 64-Bit Edition that could allow arbitrary code to run when a maliciously modified file is opened. This update resolves that vulnerability.	<a href="#">KB4493203</a>	N/A
2020-09 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	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	<a href="#">KB4576628</a>	N/A





	Base article. After you install this update, you may have to restart your system.		
Windows Malicious Software Removal Tool x64 - v5.87	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.	<a href="#"><u>KB890830</u></a>	N/A
2021-03 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.	<a href="#"><u>KB5000851</u></a>	N/A

2021-03 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 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.	<a href="#">KB5000800</a>	N/A
Security Update for Microsoft Office	This security update resolves a Microsoft Excel Remote Code Execution Vulnerability.	<a href="#">KB4504703</a>	N/A
Security Update for Microsoft Office 2010 32-Bit Edition	A security vulnerability exists in Microsoft Office 2010 32-Bit Edition that could allow arbitrary code to run when a maliciously modified file is opened. This update resolves that vulnerability.	<a href="#">KB4493214</a>	N/A
2021-02 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	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.	<a href="#">KB4603002</a>	N/A
Security Update for Microsoft Office 2010 64-Bit Edition	A security vulnerability exists in Microsoft Office 2010 64-Bit Edition that could allow arbitrary code to run when a maliciously modified file is opened. This update resolves that vulnerability. A security vulnerability exists in Microsoft Office 2010 64-Bit Edition that could allow arbitrary code to run when a maliciously modified file is opened. This update resolves that vulnerability. A security vulnerability exists in Microsoft Office 2010 64-Bit Edition that could allow arbitrary code to run when a maliciously modified file is opened. This update resolves that vulnerability.	<a href="#">KB4504703</a>	N/A

2021-03 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.	<a href="#"><u>KB5000841</u></a>	N/A
Update for Windows 7 for x64-based Systems	Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.	<a href="#"><u>KB2834140</u></a>	N/A
Update for Windows Embedded Standard 7	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.	<a href="#"><u>KB2882822</u></a>	N/A

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

Date of Critical or Security Patches: March2021

Abstract: Critical or Security Patches – March2021

### Microsoft® & Third-Party Patches

BD has identified patches from Microsoft that have been identified as critical or security related for March2021. 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
Update for Windows Embedded Standard 7 for x64-based Systems	Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.	<a href="#">KB2882822</a>	N/A
Cumulative Security Update for Internet Explorer 9 for Windows Vista 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.	<a href="#">KB3185319</a>	N/A
2021-03 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	<a href="#">KB5000841</a>	N/A



	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.		
Security Update for Windows 7 for x64-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	<a href="#">KB2868038</a>	N/A
Update for Windows Embedded Standard 7 for x64-based Systems	Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.	<a href="#">KB3138612</a>	N/A

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

Date of Critical or Security Patches - March 2021

Abstract: Critical or Security Patches - March 2021

### Microsoft® & Third-Party Patches

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

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

Patch Name	Description	Patch ID	Notes
2021-03 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems	<p>This security update resolves vulnerabilities in Internet Explorer.</p> <p>The fixes that are included in this update are also included in the March 2021 Security Monthly Quality Rollup. Installing either this update or the Security Monthly Quality Rollup installs the same fixes.</p> <p>This update is not applicable for installation on a device on which the Security Monthly Quality Rollup or the Preview of Monthly Quality Rollup from March 2021 (or a later month) is already installed. This is because those updates contain all the same fixes that are included in this update.</p> <p>If you use update management processes other than Windows Update and you automatically approve all security update classifications for deployment, this update, the March 2021 Security Only Quality Update, and the March 2021 Security Monthly</p>	<a href="#">KB5000800</a>	None



	<p>Quality Rollup are deployed. We recommend that you review your update deployment rules to make sure that the desired updates are deployed.</p> <p>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 <a href="#">Add language packs to Windows</a>.</p>		
<p>2021-03 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems</p>	<p>This security update includes improvements and fixes that were a part of update KB4601384 (released February 9, 2021) and addresses the following issues:</p> <p>Addresses an issue in which a non-native device that is in the same realm does not receive a Kerberos Service ticket from Active Directory DCs. This issue occurs even though Windows Updates are installed that contain CVE-2020-17049 protections released between November 10 and December 8, 2020 and configured PerfromTicketSignature to 1 or larger. Ticket acquisition fails with KRB_GENERIC_ERROR if callers submit a PAC-less Ticket Granting Ticket (TGT) as an evidence ticket without the USER_NO_AUTH_DATA_REQUIRED flag being set for the user in User Account Controls.</p>	<p><a href="#">KB5000848</a></p>	<p>None</p>

	<p>Addresses an elevation of privilege security vulnerability documented in CVE-2021-1640 related to print jobs submitted to "FILE:" ports. After installing Windows updates from March 9, 2021 and later, print jobs that are in a pending state before restarting the print spooler service or restarting the OS will remain in an error state. Manually delete the affected print jobs and resubmit them to the print queue when the print spooler service is online.</p> <p>Security updates to Windows Fundamentals, Windows Shell, Windows UAC, Windows Hybrid Cloud Networking, Windows Media, and Windows Graphics.</p>		
<p>2021-03 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems</p>	<p>This security update includes quality improvements. Key changes include:</p> <p>Addresses an issue in which a non-native device that is in the same realm does not receive a Kerberos Service ticket from Active Directory DCs. This issue occurs even though Windows Updates are installed that contain CVE-2020-17049 protections released between November 10 and December 8, 2020 and configured PerfromTicketSignature to 1 or larger. Ticket acquisition fails with KRB_GENERIC_ERROR if callers submit a PAC-less Ticket Granting Ticket (TGT) as an evidence ticket without the USER_NO_AUTH_DATA_REQUIRED flag being set for the</p>	<p><a href="#">KB5000853</a></p>	<p>None</p>



	<p>user in User Account Controls.</p> <p>Security updates to Windows Fundamentals, Windows Shell, Windows UAC, Windows Hybrid Cloud Networking, Windows Media, and Windows Graphics.</p>		
<p>2021-03 Security Only Quality Update for Windows Embedded Standard 7 for x64-based Systems</p>	<p>This security update includes quality improvements. Key changes include:</p> <p>Addresses an issue in which a non-native device that is in the same realm does not receive a Kerberos Service ticket from Active Directory DCs. This issue occurs even though Windows Updates are installed that contain CVE-2020-17049 protections released between November 10 and December 8, 2020 and configured PerfromTicketSignature to 1 or larger. Ticket acquisition fails with KRB_GENERIC_ERROR if callers submit a PAC-less Ticket Granting Ticket (TGT) as an evidence ticket without the USER_NO_AUTH_DATA_REQUIRED flag being set for the user in User Account Controls.</p> <p>Security updates to Windows Fundamentals, Windows Shell, Windows UAC, Windows Hybrid Cloud Networking, and Windows Media.</p>	<p><a href="#">KB5000851</a></p>	<p>None</p>

<p>2021-03 Cumulative Update for Windows 10 Version 1607 for x64-based Systems</p>	<p>Updates security for the Windows user interface.</p> <p>Updates to improve security when Windows performs basic operations.</p> <p>Updates to improve security when using Microsoft Office products.</p>	<p><a href="#">KB5000803</a></p>	<p>None</p>
<p>2021-01 Update for Windows Server 2016 for x64-based Systems</p>	<p>This update is a standalone update that is targeted at Windows 10, version 1607 and Windows Server 2016. This update also includes Intel microcode updates that were already released for these operating systems at the time of release. We will offer additional microcode updates from Intel through this article for these operating systems as they become available to Microsoft. Use the registry settings as described in the Windows client and Windows Server KB articles.</p>	<p><a href="#">KB4589210</a></p>	<p>None</p>
<p>2021-03 Cumulative Update for Windows 10 Version 1809 for x64-based Systems</p>	<p>This security update Addresses an elevation of privilege security vulnerability documented in CVE-2021-1640 related to print jobs submitted to "FILE:" ports. After installing Windows updates from March 9, 2021 and later, print jobs that are in a pending state before restarting the print spooler service or restarting the OS will remain in an error state. Manually delete the affected print jobs and resubmit them to the print queue when the print spooler service is online.</p> <p>Security updates to the Windows Shell, Windows Fundamentals, Windows</p>	<p><a href="#">KB5000822</a></p>	<p>None</p>

	Management, Windows Apps, Windows User Account Control (UAC), Windows Core Networking, Windows Hybrid Cloud Networking, the Windows Kernel, Windows Virtualization, the Microsoft Graphics Component, Internet Explorer, Microsoft Edge Legacy, and Windows Media.		
Update for Removal of Adobe Flash Player for Windows 10 Version 1803 for x64-based systems	This update removes Adobe Flash Player that is installed on any of the Windows operating systems that are listed in the "Applies to" section. After you apply this update, it cannot be uninstalled.	<a href="#">KB4577586</a>	None
Windows Malicious Software Removal Tool x64 -v5.87	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	<a href="#">KB890830</a>	None
Security Update for Microsoft windows	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.	<a href="#">KB5000859</a>	None

2021-03 Cumulative Update for Windows 10	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.	<a href="#">KB5000822</a>	None
--	--	---------------------------	------

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

Date of Critical or Security Patches - March 2021

Abstract: Critical or Security Patches - March 2021

### Microsoft® & Third-Party Patches

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

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

Patch Name	Description	Patch ID	Notes
2021-03 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems	<p>This security update resolves vulnerabilities in Internet Explorer.</p> <p>The fixes that are included in this update are also included in the March 2021 Security Monthly Quality Rollup. Installing either this update or the Security Monthly Quality Rollup installs the same fixes.</p> <p>This update is not applicable for installation on a device on which the Security Monthly Quality Rollup or the Preview of Monthly Quality Rollup from March 2021 (or a later month) is already installed. This is because those updates contain all the same fixes that are included in this update.</p> <p>If you use update management processes other than Windows Update and you automatically approve all security update classifications for deployment, this update, the March 2021 Security Only Quality Update, and the March 2021 Security Monthly</p>	<a href="#">KB5000800</a>	None



	<p>Quality Rollup are deployed. We recommend that you review your update deployment rules to make sure that the desired updates are deployed.</p> <p>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 <a href="#">Add language packs to Windows</a>.</p>		
<p>2021-03 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems</p>	<p>This security update includes improvements and fixes that were a part of update KB4601384 (released February 9, 2021) and addresses the following issues:</p> <p>Addresses an issue in which a non-native device that is in the same realm does not receive a Kerberos Service ticket from Active Directory DCs. This issue occurs even though Windows Updates are installed that contain CVE-2020-17049 protections released between November 10 and December 8, 2020 and configured PerfromTicketSignature to 1 or larger. Ticket acquisition fails with KRB_GENERIC_ERROR if callers submit a PAC-less Ticket Granting Ticket (TGT) as an evidence ticket without the USER_NO_AUTH_DATA_REQUIRED flag being set for the user in User Account Controls.</p>	<p><a href="#">KB5000848</a></p>	<p>None</p>

	<p>Addresses an elevation of privilege security vulnerability documented in CVE-2021-1640 related to print jobs submitted to "FILE:" ports. After installing Windows updates from March 9, 2021 and later, print jobs that are in a pending state before restarting the print spooler service or restarting the OS will remain in an error state. Manually delete the affected print jobs and resubmit them to the print queue when the print spooler service is online.</p> <p>Security updates to Windows Fundamentals, Windows Shell, Windows UAC, Windows Hybrid Cloud Networking, Windows Media, and Windows Graphics.</p>		
<p>2021-03 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems</p>	<p>This security update includes quality improvements. Key changes include:</p> <p>Addresses an issue in which a non-native device that is in the same realm does not receive a Kerberos Service ticket from Active Directory DCs. This issue occurs even though Windows Updates are installed that contain CVE-2020-17049 protections released between November 10 and December 8, 2020 and configured PerfromTicketSignature to 1 or larger. Ticket acquisition fails with KRB_GENERIC_ERROR if callers submit a PAC-less Ticket Granting Ticket (TGT) as an evidence ticket without the USER_NO_AUTH_DATA_REQUIRED flag being set for the</p>	<p><a href="#">KB5000853</a></p>	<p>None</p>

	<p>user in User Account Controls.</p> <p>Security updates to Windows Fundamentals, Windows Shell, Windows UAC, Windows Hybrid Cloud Networking, Windows Media, and Windows Graphics.</p>		
<p>2021-03 Security Only Quality Update for Windows Embedded Standard 7 for x64-based Systems</p>	<p>This security update includes quality improvements. Key changes include:</p> <p>Addresses an issue in which a non-native device that is in the same realm does not receive a Kerberos Service ticket from Active Directory DCs. This issue occurs even though Windows Updates are installed that contain CVE-2020-17049 protections released between November 10 and December 8, 2020 and configured PerfromTicketSignature to 1 or larger. Ticket acquisition fails with KRB_GENERIC_ERROR if callers submit a PAC-less Ticket Granting Ticket (TGT) as an evidence ticket without the USER_NO_AUTH_DATA_REQUIRED flag being set for the user in User Account Controls.</p> <p>Security updates to Windows Fundamentals, Windows Shell, Windows UAC, Windows Hybrid Cloud Networking, and Windows Media.</p>	<p><a href="#">KB5000851</a></p>	<p>None</p>



<p>2021-03 Cumulative Update for Windows 10 Version 1607 for x64-based Systems</p>	<p>Updates security for the Windows user interface.</p> <p>Updates to improve security when Windows performs basic operations.</p> <p>Updates to improve security when using Microsoft Office products.</p>	<p><a href="#">KB5000803</a></p>	<p>None</p>
<p>2021-01 Update for Windows Server 2016 for x64-based Systems</p>	<p>This update is a standalone update that is targeted at Windows 10, version 1607 and Windows Server 2016. This update also includes Intel microcode updates that were already released for these operating systems at the time of release. We will offer additional microcode updates from Intel through this article for these operating systems as they become available to Microsoft. Use the registry settings as described in the Windows client and Windows Server KB articles.</p>	<p><a href="#">KB4589210</a></p>	<p>None</p>
<p>2021-03 Cumulative Update for Windows 10 Version 1809 for x64-based Systems</p>	<p>This security update Addresses an elevation of privilege security vulnerability documented in CVE-2021-1640 related to print jobs submitted to "FILE:" ports. After installing Windows updates from March 9, 2021 and later, print jobs that are in a pending state before restarting the print spooler service or restarting the OS will remain in an error state. Manually delete the affected print jobs and resubmit them to the print queue when the print spooler service is online.</p> <p>Security updates to the Windows Shell, Windows Fundamentals, Windows</p>	<p><a href="#">KB5000822</a></p>	<p>None</p>

	Management, Windows Apps, Windows User Account Control (UAC), Windows Core Networking, Windows Hybrid Cloud Networking, the Windows Kernel, Windows Virtualization, the Microsoft Graphics Component, Internet Explorer, Microsoft Edge Legacy, and Windows Media.		
Update for Removal of Adobe Flash Player for Windows 10 Version 1803 for x64-based systems	This update removes Adobe Flash Player that is installed on any of the Windows operating systems that are listed in the "Applies to" section. After you apply this update, it cannot be uninstalled.	<a href="#">KB4577586</a>	None
Windows Malicious Software Removal Tool x64 -v5.87	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	<a href="#">KB890830</a>	None
Security Update for Microsoft windows	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.	<a href="#">KB5000859</a>	None

2021-03 Cumulative Update for Windows 10	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.	<a href="#">KB5000822</a>	None
--	--	---------------------------	------