Security Patches: BD Pyxis™ Anesthesia ES

April 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for April 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.99	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	Applicable on PAS device.

2022-04 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 KB5011552 (released March 8, 2022) and addresses the following issues: Addresses an issue in Windows Media Center where some users might have to reconfigure the application on each start. Addresses a memory leak that was introduced by the PacRequestorEnforcement registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain controllers. Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. Addresses an issue that occurs when you try to write a service principal name (SPN) alias (such as www/contoso) and HOST/NAME already exists on another object. If the user has the RIGHT_DS_WRITE_PROPERTY on the SPN attribute of the colliding object, you receive an “Access Denied” error.Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames. Addresses an issue that prevents you from changing a password that has expired when you sign in to a Windows device.	KB5012626	Applicable on PAS device.
2022-04 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 Windows Media Center where some users might have to reconfigure the application on each start. Addresses a memory leak that was introduced by the PacRequestorEnforcement registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain controllers. Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. Windows Malicious Software Removal Tool x64 - v5.100If the user has the RIGHT_DS_WRITE_PROPERTY on the SPN attribute of the colliding object, you receive an “Access Denied” error. Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames.	KB5012649	Applicable on PAS device.

Windows Malicious Software Removal Tool x64 - v5.100	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on PAS device.
2022-04 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.	**KB5012647**	Applicable on PAS device.
2022-04 Cumulative Update for Windows 10 Version 1607 for x64-based Systems.	This security update includes quality improvements. Key changes include: Addresses a heap leak in PacRequestorEnforcement that degrades the performance of a domain controller. Addresses an issue that affects the Key Distribution Center (KDC) Proxy. The KDC Proxy cannot properly obtain Kerberos tickets for signing in to Key Trust Windows Hello for Business. Addresses an issue that logs Event ID 37 during certain password change scenarios, including failover cluster name object (CNO) or virtual computer object (VCO) password changes. Addresses an issue that causes a Denial of Service vulnerability on Cluster Shared Volumes (CSV). For more information, see CVE-2020-26784. Addresses an issue that prevents you from changing a password that has expired when you sign in to a Windows device.	KB5012596	Applicable on PAS device.

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

bd.com

Security Patches:
BD Pyxis™ Med Station ES

April 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for April 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.99	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	Applicable on MedSTN device.

2022-04 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 KB5011552 (released March 8, 2022) and addresses the following issues: Addresses an issue in Windows Media Center where some users might have to reconfigure the application on each start. Addresses a memory leak that was introduced by the PacRequestorEnforcement registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain controllers. Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. Addresses an issue that occurs when you try to write a service principal name (SPN) alias (such as www/contoso) and HOST/NAME already exists on another object. If the user has the RIGHT_DS_WRITE_PROPERTY on the SPN attribute of the colliding object, you receive an “Access Denied” error.Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames. Addresses an issue that prevents you from changing a password that has expired when you sign in to a Windows device.	KB5012626	Applicable on MedSTN device.
2022-04 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	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.	KB5012329	Applicable on MedSTN device.
2022-04 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5012626	Applicable on MedSTN device.
2022-04 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5012649	Applicable on MedSTN device.

2022-04 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.	KB5012649	Applicable on MedSTN device.
2022-04 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.	KB5012639	Applicable on MedSTN device.
2022-04 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.	KB5012670	Applicable on MedSTN device.
2022-04 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems	Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.	KB5012672	Applicable on MedSTN device.

Windows Malicious Software Removal Tool x64 - v5.100	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	Applicable on MedSTN device.
2022-04 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.	KB5012647	Applicable on MedSTN device.
2022-04 Cumulative Update for Windows 10 Version 1607 for x64-based Systems.	This security update includes quality improvements. Key changes include: Addresses a heap leak in PacRequestorEnforcement that degrades the performance of a domain controller. Addresses an issue that affects the Key Distribution Center (KDC) Proxy. The KDC Proxy cannot properly obtain Kerberos tickets for signing in to Key Trust Windows Hello for Business. Addresses an issue that logs Event ID 37 during certain password change scenarios, including failover cluster name object (CNO) or virtual computer object (VCO) password changes. Addresses an issue that causes a Denial of Service vulnerability on Cluster Shared Volumes (CSV). For more information, see CVE-2020-26784. Addresses an issue that prevents you from changing a password that has expired when you sign in to a Windows device.	KB5012596	Applicable on MedSTN device.

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

bd.com

Security Patches: BD Pyxis CIISafe

April 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for April 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
2022-04 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x64-based Systems (KB5012626)	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.	KB5012626	Applicable on CII Safe.
Windows Malicious Software Removal Tool x64 - v5.100 (KB890830)	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	Applicable on CII Safe.

2022-04 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 (KB5012329)	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.	KB5012329	Applicable on CIISafe.

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

bd.com

Security Patches: BD Pyxis™ Supply

April 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for April 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
2022-04 Security Only Quality Update for Windows Embedded Standard 7 for x64-based Systems (KB5012649)	This security update includes quality improvements. Key changes include: • Addresses an issue in Windows Media Center where some users might have to reconfigure the application on each start. • Addresses a memory leak that was introduced by the PacRequestorEnforcement registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain controllers. • Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. • Addresses an issue that occurs when you try to write a service principal name (SPN) alias (such as www/contoso) and HOST/NAME already exists on another object. If the user has the RIGHT_DS_WRITE_PROPERTY on the SPN attribute of the colliding object, you receive an "Access Denied" error. • Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames.	KB5012649	Applicable on Supply.

2022-04 Security Only Quality Update for Windows Server 2008 R2 for x64-based Systems (KB5012649)	This security update includes quality improvements. Key changes include: • Addresses an issue in Windows Media Center where some users might have to reconfigure the application on each start. • Addresses a memory leak that was introduced by the PacRequestorEnforcement registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain controllers. • Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. • Addresses an issue that occurs when you try to write a service principal name (SPN) alias (such as www/contoso) and HOST/NAME already exists on another object. If the user has the RIGHT_DS_WRITE_PROPERTY on the SPN attribute of the colliding object, you receive an “Access Denied” error. • Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames.	KB5012649	Applicable on Supply.

2022-04 Security Monthly Quality Rollup for Windows Embedded Standard 7 for x86-based Systems (KB5012626)	This security update includes improvements and fixes that were a part of update KB5011552 (released March 8, 2022) and addresses the following issues: • Addresses an issue in Windows Media Center where some users might have to reconfigure the application on each start. • Addresses a memory leak that was introduced by the PacRequestorEnforcement registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain controllers. • Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. • Addresses an issue that occurs when you try to write a service principal name (SPN) alias (such as www/contoso) and HOST/NAME already exists on another object. If the user has the RIGHT_DS_WRITE_PROPERTY on the SPN attribute of the colliding object, you receive an “Access Denied” error. • Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames. • Addresses an issue that prevents you from changing a password that has expired when you sign in to a Windows device.	KB5012626	Applicable on Supply.

2022-04 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5012596)	This security update includes quality improvements. Key changes include: • Addresses a heap leak in PacRequestorEnforcement that degrades the performance of a domain controller. • Addresses an issue that affects the Key Distribution Center (KDC) Proxy. The KDC Proxy cannot properly obtain Kerberos tickets for signing in to Key Trust Windows Hello for Business. • Addresses an issue that logs Event ID 37 during certain password change scenarios, including failover cluster name object (CNO) or virtual computer object (VCO) password changes. • Addresses an issue that causes a Denial of Service vulnerability on Cluster Shared Volumes (CSV). For more information, see CVE-2020-26784. • Addresses an issue that prevents you from changing a password that has expired when you sign in to a Windows device.	KB5012596	Applicable on Supply.
2022-04 Cumulative Update for Windows Server 2019 for x64-based Systems (KB5012647)	This security update includes improvements that were a part of update KB5011551 (released March 15, 2022) and also addresses the following issues: • Addresses a known issue that causes DNS stub load failures on a Windows Server that is running a DNS Server. • Addresses an issue that causes a Denial of Service vulnerability on Cluster Shared Volumes (CSV). For more information, see CVE-2020-26784. • Addresses an issue that prevents you from changing a password that has expired when you sign in to a Windows device.	KB5012647	Applicable on Supply.
2022-04 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB5012647)	This security update includes improvements that were a part of update KB5011551 (released March 15, 2022) and also addresses the following issues: • Addresses a known issue that causes DNS stub load failures on a Windows Server that is running a DNS Server. • Addresses an issue that causes a Denial of Service vulnerability on Cluster Shared Volumes (CSV). For more information, see CVE-2020-26784. • Addresses an issue that prevents you from changing a password that has expired when you sign in to a Windows device.	KB5012647	Applicable on Supply.

2022-04 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows Server 2019 for x64 (KB5012119)	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-2022-26832.	KB5012119	Applicable on Supply.
2022-04 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 (KB5012328)	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-2022-26832.	KB5012328	Applicable on Supply.
Windows Malicious Software Removal Tool x64 - v5.100	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers. Microsoft releases the MSRT on a monthly cadence as part of Windows Update or as a standalone tool. Use this tool to find and remove specific prevalent threats and reverse the changes they have made.	KB890830	Applicable on Supply.

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

bd.com

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

April 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for April 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
2022-01 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	Applicable on CIIsafe device.
2022-03 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.	KB5011503	Applicable on CIIsafe device.

2022-04 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.	KB5012647	Applicable on CIIsafe device.
Windows Malicious Software Removal Tool x64 - v5.99	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	Applicable on CIIsafe device.
2022-04 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.	KB5012647	Applicable on CIIsafe device.

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

bd.com

Security Patches: BD Pharmogistics

April 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for April 2022. These patches were not found to adversely affect BD Pharmogistics products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	Applicable on PLX, CII Safe and Infusion.
2022-04 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB5012672) Last Modified: 4/12/2022	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates. Additionally, this update address an issue in which Windows might go into BitLocker recovery after a servicing update.	KB5012672	N/A

2022-04 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5012670)	KB5012670 is a monthly rollup update for April 2022. It supersedes the March month's monthly rollup update for Windows Server 2012 R2 – KB5011564. The monthly rollup update contains all the changes that are part of the security-only update for April 2022 for Windows Server 2012 R2. In other words, the KB5012670 monthly rollup update contains all the changes that are part of the KB5012639 security-only updat	KB5012670	N/A
2022-04 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5012639) Last Modified: 4/8/2022	This security update includes quality improvements. Key changes include: Addresses an issue in Windows Media Center where some users might have to reconfigure the application on each start. Addresses a memory leak that was introduced by the PacRequestorEnforcement registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain controllers. Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames.	KB5012639	N/A
2022-04 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 21H2 for x64 (KB5012117) Last Modified: 4/8/2022	Security Improvements 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-2022-26832.	KB5012117	N/A

2022-04 Update for Windows 10 Version 1803 for x64-based Systems (KB4023057)	This update includes reliability improvements to Windows Update Service components in all editions of Windows 10, version 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, 21H1, 21H2, and Windows 11 (original release). It may take steps to free up disk space on your device if you do not have enough disk space to install Windows updates.	KB4023057	N/A
2022-04 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5012596)	This security update includes quality improvements. Key changes include: Addresses a heap leak in PacRequestorEnforcement that degrades the performance of a domain controller. Addresses an issue that affects the Key Distribution Center (KDC) Proxy. The KDC Proxy cannot properly obtain Kerberos tickets for signing in to Key Trust Windows Hello for Business. Addresses an issue that logs Event ID 37 during certain password change scenarios, including failover cluster name object (CNO) or virtual computer object (VCO) password changes.	KB5012596	N/A

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

bd.com

Security Patches: BD Pyxis Connect

April 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for April 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.100	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	
2022-04 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 (KB5012331)	This security update addresses an issue where an unauthenticated attacker could cause a denial of service on an affected system.	KB5012331	

2022-04 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB5012672)	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. Additionally, this update address an issue in which Windows might go into BitLocker recovery after a servicing update.	KB5012672
2022-04 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5012670)	This security update includes improvements and fixes that were a part of update KB5011564 (released March 8, 2022) and addresses the following issues: Addresses an issue in Windows Media Center where some users might have to reconfigure the application on each start. Addresses a memory leak that was introduced by the PacRequestorEnforcement registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain controllers. Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. Addresses an issue in which Windows might go into BitLocker recovery after a servicing update. Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames.	KB5012670
2022-04 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5012639)	This security update includes quality improvements. Key changes include: ▪ Addresses an issue in Windows Media Center where some users might have to reconfigure the application on each start. ▪ Addresses a memory leak that was introduced by the PacRequestorEnforcement registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain controllers. ▪ Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. ▪ Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames.	KB5012639

2022-04 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5012596)	This security update includes quality improvements. Key changes include: ▪ Addresses a heap leak in PacRequestorEnforcement that degrades the performance of a domain controller. ▪ Addresses an issue that affects the Key Distribution Center (KDC) Proxy. The KDC Proxy cannot properly obtain Kerberos tickets for signing in to Key Trust Windows Hello for Business. ▪ Addresses an issue that logs Event ID 37 during certain password change scenarios, including failover cluster name object (CNO) or virtual computer object (VCO) password changes. ▪ Addresses an issue that causes a Denial of Service vulnerability on Cluster Shared Volumes (CSV). ▪ Addresses an issue that prevents you from changing a password that has expired when you sign in to a Windows device.	KB5012596
2022-04 Cumulative Update for Windows 10 Version 21H1 for x64-based Systems (KB5012599)	▪ Updates security for your Windows operating system.	KB5012599
2022-04 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 21H1 for x64 (KB5012117)	Addresses a leak of IRawElementProviderSimple objects which was introduced in .NET Framework 4.8.	KB5012117

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

bd.com

Security Patches: BD Pyxis Parx

Apr 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for April 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.99	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	Applicable to Parx device

2022-04 Cumulative Update for Windows 10 Version 1607 for x64-based Systems	Updates an issue that prevents you from changing a password that has expired when you sign in to a Windows device.Updates security for your Windows operating system.	KB5012596	Applicable to Parx device

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

bd.com

Security Patches: BD Pyxis™ IV Prep

April 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for April 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.100	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	Applicable on Cato
2022-04 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.	KB5012639	Applicable on Cato

2022-04 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.	KB5012670	Applicable on Cato
2022-04 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 Knowledge Base article. After you install this update, you may have to restart your system.	KB5012331	Applicable on Cato
2022-04 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems	Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.	KB5012672	Applicable on Cato
2022-04 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. After you install this update, you may have to restart your system.	KB5012124	Applicable on Cato
2022-04 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. After you install this update, you may have to restart your system.	KB5012139	Applicable on Cato
2022-04 Cumulative Update for Windows Server 2016 for x64-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5012596	Applicable on Cato

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

bd.com

Security Patches: BD Pyxis™ MedStation™ 4000

April 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for April 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.100	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS4000 Console, Anesthesia System and Station
2022-04 Cumulative Update for Windows Server 2016 for x64-based Systems.	This security update includes quality improvements. Key changes include: Addresses a heap leak in PacRequestorEnforcement that degrades the performance of a domain controller. Addresses an issue that affects the Key Distribution Center (KDC) Proxy. The KDC Proxy cannot properly obtain Kerberos tickets for signing in to Key Trust Windows Hello for Business. Addresses an issue that logs Event ID 37 during certain password change scenarios, including failover cluster name object (CNO) or virtual computer object (VCO) password changes. Addresses an issue that causes a Denial of Service vulnerability on Cluster Shared Volumes (CSV). For more information, see CVE-2020-26784. Addresses an issue that prevents you from changing a password that has expired when you sign in to a Windows device.	KB5012596	Applicable on MS4000 Console

2022-04 Cumulative Update for Windows 10 Version 1607 for x64-based Systems.	This security update includes quality improvements. Key changes include: Addresses a heap leak in PacRequestorEnforcement that degrades the performance of a domain controller. Addresses an issue that affects the Key Distribution Center (KDC) Proxy. The KDC Proxy cannot properly obtain Kerberos tickets for signing in to Key Trust Windows Hello for Business. Addresses an issue that logs Event ID 37 during certain password change scenarios, including failover cluster name object (CNO) or virtual computer object (VCO) password changes. Addresses an issue that causes a Denial of Service vulnerability on Cluster Shared Volumes (CSV). For more information, see CVE-2020-26784. Addresses an issue that prevents you from changing a password that has expired when you sign in to a Windows device.	KB5012596	Applicable on MS4000 Anesthesia System and Station
Windows Malicious Software Removal Tool - v5.100	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS4000 Console, Anesthesia System and Station
2022-04 Security Only Quality Update for Windows Server 2008 for x86-based Systems	This security update includes quality improvements. Key changes include: Addresses a memory leak that was introduced by the PacRequestorEnforcement registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain controllers. Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames.	KB5012632	Applicable on MS4000 Console and MED3500 Console
2022-04 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 KB5011534 (released March 8, 2022) and addresses the following issues: Addresses a memory leak that was introduced by the PacRequestorEnforcement registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain controllers. Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames. Addresses an issue that prevents you from changing a password that has expired when you sign in to a Windows device.	KB5012658	Applicable on MS4000 Console and MED3500 Console

2022-04 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 Windows Media Center where some users might have to reconfigure the application on each start. Addresses a memory leak that was introduced by the PacRequestorEnforcement registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain controllers. Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. Addresses an issue that occurs when you try to write a service principal name (SPN) alias (such as www/contoso) and HOST/NAME already exists on another object. If the user has the RIGHT_DS_WRITE_PROPERTY on the SPN attribute of the colliding object, you receive an “Access Denied” error. Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames.	KB5012649	Applicable on Station and Anesthesia system
2022-04 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 KB5011552 (released March 8, 2022) and addresses the following issues: Addresses an issue in Windows Media Center where some users might have to reconfigure the application on each start. Addresses a memory leak that was introduced by the PacRequestorEnforcement registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain controllers. Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. Addresses an issue that occurs when you try to write a service principal name (SPN) alias (such as www/contoso) and HOST/NAME already exists on another object. If the user has the RIGHT_DS_WRITE_PROPERTY on the SPN attribute of the colliding object, you receive an “Access Denied” error. Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames. Addresses an issue that prevents you from changing a password that has expired when you sign in to a Windows device.	KB5012626	Applicable on Station and Anesthesia system

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

bd.com

Security Patches: BD Pyxis™ MedStation™ 3500

April 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for April 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
2022-04 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 Windows Media Center where some users might have to reconfigure the application on each start. Addresses a memory leak that was introduced by the PacRequestorEnforcement registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain controllers. Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. Addresses an issue that occurs when you try to write a service principal name (SPN) alias (such as www/contoso) and HOST/NAME already exists on another object. If the user has the RIGHT_DS_WRITE_PROPERTY on the SPN attribute of the colliding object, you receive an "Access Denied" error. Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames.	KB5012649	Applicable on MS3500 Station, MS3500 Anesthesia System and Med4000 windows 7.
2022-04 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 KB5011552 (released March 8, 2022) and addresses the following issues: Addresses an issue in Windows Media Center where some users might have to reconfigure the application on each start. Addresses a memory leak that was introduced by the PacRequestorEnforcement registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain	KB5012626	Applicable on MS3500 Station, MS3500 Anesthesia System and Med4000 windows 7.

	controllers. Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. Addresses an issue that occurs when you try to write a service principal name (SPN) alias (such as www/contoso) and HOST/NAME already exists on another object. If the user has the RIGHT_DS_WRITE_PROPERTY on the SPN attribute of the colliding object, you receive an “Access Denied” error. Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames. Addresses an issue that prevents you from changing a password that has expired when you sign in to a Windows device.		
2022-04 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 KB5011534 (released March 8, 2022) and addresses the following issues: Addresses a memory leak that was introduced by the PacRequestorEnforcement registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain controllers. Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames. Addresses an issue that prevents you from changing a password that has expired when you sign in to a Windows device.	KB5012658	Applicable on MS3500 and MS 4000 Console
2022-04 Security Only Quality Update for Windows Server 2008 for x86-based Systems	This security update includes quality improvements. Key changes include: Addresses a memory leak that was introduced by the PacRequestorEnforcement registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain controllers. Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames.	KB5012632	Applicable on MS3500 and MS 4000 Console
Windows Malicious Software Removal Tool - v5.100	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS3500 and MS 4000 Console

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

bd.com

Security Patches: BD Pyxis™ Anesthesia System 4000

April 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for April 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.100	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	Applicable on MS4000 Console, Anesthesia System and Station
2022-04 Cumulative Update for Windows 10 Version 1607 for x64-based Systems.	This security update includes quality improvements. Key changes include: Addresses a heap leak in PacRequestorEnforcement that degrades the performance of a domain controller. Addresses an issue that affects the Key Distribution Center (KDC) Proxy. The KDC Proxy cannot properly obtain Kerberos tickets for signing in to Key Trust Windows Hello for Business. Addresses an issue that logs Event ID 37 during certain password change scenarios, including failover cluster name object (CNO) or virtual computer object (VCO) password changes. Addresses an issue that causes a Denial of Service vulnerability on Cluster Shared Volumes (CSV). For more information, see CVE-2020-26784. Addresses an issue that prevents you from changing a password that has expired when you sign in to a Windows device.	KB5012596	Applicable on Anesthesia System and MS4000
2022-04 Security Only Quality Update for Windows	This security update includes quality improvements. Key changes include: Addresses an issue in Windows	KB5012649	

Embedded Standard 7 for x86-based Systems.	Media Center where some users might have to reconfigure the application on each start. Addresses a memory leak that was introduced by the PacRequestorEnforcement registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain controllers. Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. Addresses an issue that occurs when you try to write a service principal name (SPN) alias (such as www/contoso) and HOST/NAME already exists on another object. If the user has the RIGHT_DS_WRITE_PROPERTY on the SPN attribute of the colliding object, you receive an “Access Denied” error. Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames.		Applicable on Anesthesia System and Station
2022-04 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 KB5011552 (released March 8, 2022) and addresses the following issues: Addresses an issue in Windows Media Center where some users might have to reconfigure the application on each start. Addresses a memory leak that was introduced by the PacRequestorEnforcement registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain controllers. Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. Addresses an issue that occurs when you try to write a service principal name (SPN) alias (such as www/contoso) and HOST/NAME already exists on another object. If the user has the RIGHT_DS_WRITE_PROPERTY on the SPN attribute of the colliding object, you receive an “Access Denied” error.Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames. Addresses an issue that prevents you from changing a password that has expired when you sign in to a Windows device.	KB5012626	Applicable on Anesthesia System and Station

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

Security Patches: BD Pyxis™ Anesthesia System 3500

April 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for April 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
2022-04 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 KB5011552 (released March 8, 2022) and addresses the following issues: Addresses an issue in Windows Media Center where some users might have to reconfigure the application on each start. Addresses a memory leak that was introduced by the PacRequestorEnforcement registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain controllers. Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. Addresses an issue that occurs when you try to write a service principal name (SPN) alias (such as www/contoso) and HOST/NAME already exists on another object. If the user has the RIGHT_DS_WRITE_PROPERTY on the SPN attribute of the colliding object, you receive an "Access Denied" error. Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames. Addresses an issue that prevents you from changing a password that has expired when you sign into a Windows device.	KB5012626	Applicable on 3500 Anesthesia System and MS3500 Station

2022-04 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 Windows Media Center where some users might have to reconfigure the application on each start. Addresses a memory leak that was introduced by the PacRequestorEnforcement registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain controllers. Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. Addresses an issue that occurs when you try to write a service principal name (SPN) alias (such as www/contoso) and HOST/NAME already exists on another object. If the user has the RIGHT_DS_WRITE_PROPERTY on the SPN attribute of the colliding object, you receive an “Access Denied” error. Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames.	KB5012649	Applicable on 3500 Anesthesia System and MS3500 Station

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

bd.com

Security Patches: Security Module

April 2022

BD has identified patches from Microsoft® that have been identified as critical or security related for April 2022. These patches were not found to adversely affect BD products and will be applied according to customers' service agreements.

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

Microsoft® patches

Patch name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.100 (KB890830)	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	KB890830	N/A

2022-04 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5012639)	This security update includes quality improvements. Key changes include: ▪Addresses an issue in Windows Media Center where some users might have to reconfigure the application on each start. ▪Addresses a memory leak that was introduced by the PacRequestorEnforcement registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain controllers. ▪Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. ▪Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames.	KB5012639	N/A
2022-04 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5012670)	This security update includes improvements and fixes that were a part of update KB5011564 (released March 8, 2022) and addresses the following issues: ▪Addresses an issue in Windows Media Center where some users might have to reconfigure the application on each start. ▪Addresses a memory leak that was introduced by the PacRequestorEnforcement registry key in the November 2021 Cumulative Update that causes a decrease in performance on domain controllers. ▪Addresses an issue in which Event ID 37 might be logged during certain password change scenarios. ▪Addresses an issue in which Windows might go into BitLocker recovery after a servicing update. ▪Addresses an issue in which domain joins may fail in environments that use disjoint DNS hostnames. ▪Addresses an issue that causes a Denial of Service vulnerability on Cluster Shared Volumes (CSV). For more information, see CVE-2020-26784. ▪Addresses an issue that prevents you from changing a password that has expired when you sign in to a Windows device.	KB5012670	N/A

2022-04 Servicing Stack Update for Windows Server 2012 R2 for x64-based Systems (KB5012672)	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. Additionally, this update address an issue in which Windows might go into BitLocker recovery after a servicing update. This update applies to the following: ▪Windows 8.1 for x86-based devices ▪Windows 8.1 for x64-based devices ▪Windows RT 8.1 ▪Windows Server 2012 R2 ▪Windows Server 2012 R2 (Server Core installation)	KB5012672	N/A
2022-04 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5012596)	This security update includes quality improvements. Key changes include: ▪Addresses a heap leak in PacRequestorEnforcement that degrades the performance of a domain controller. ▪Addresses an issue that affects the Key Distribution Center (KDC) Proxy. The KDC Proxy cannot properly obtain Kerberos tickets for signing in to Key Trust Windows Hello for Business. ▪Addresses an issue that logs Event ID 37 during certain password change scenarios, including failover cluster name object (CNO) or virtual computer object (VCO) password changes. ▪Addresses an issue that causes a Denial of Service vulnerability on Cluster Shared Volumes (CSV). For more information, see CVE-2020-26784. ▪Addresses an issue that prevents you from changing a password that has expired when you sign in to a Windows device.	KB5012596	N/A

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

bd.com