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

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

Microsoft® & Third-Party Patches

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

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

Patch Name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.98	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	N/A
2022-02 Cumulative Update for Windows 10 Version 1607 for x64-based Systems.	This security update includes quality improvements. Key changes include: Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. Updates the phone number for Windows Activation for locales that have the wrong phone number. Addresses an issue that causes Windows to stop working and generates the error, "IRQL_NOT_LESS_OR_EQUAL". Addresses an issue that causes the improper cleanup of Dynamic Data Exchange (DDE) objects. This prevents session teardown and causes a session to stop responding. Addresses an access violation in IKEEXT.dll that occurs on Always On VPN (AOVPN) and DirectAccess servers. The exception code is 0xC000005. Addresses an issue that affects Administrative Template settings you configure using a Group Policy Object (GPO). When you change the value of the policy setting to NOT CONFIGURED, the system fails to remove the previous setting. This issue is most noticeable for roaming user profiles.	KB5010359	N/A

	Addresses a memory leak that occurs when you call WinVerifyTrust(). This issue occurs if verification fails for the first signature of a file that has multiple signatures. Addresses a known issue that affects versions of Windows Server that are in use as a Key Management Services (KMS) host. Client devices running Windows 10 Enterprise LTSC 2016 might not activate. This issue only occurs when using a new Customer Support Volume License Key (CSVLK) and after installing updates released April 22, 2021 or later. Adds an audit event to Active Directory domain controllers that identifies clients that are not compliant with RFC 4456. For more information, see KB5005408: Smart card authentication might cause print and scan failures. Addresses an issue that might cause Kerberos.dll to stop working within the Local Security Authority Subsystem Service (LSASS). This occurs when LSASS processes simultaneous Service for User (S4U) user-to-user (U2U) requests for the same client user. Addresses an issue that causes a Lightweight Directory Access Protocol (LDAP) modify operation to fail if the operation contains the SamAccountName and UserAccountControl attributes. The error message is, "Error: 0x20EF. The directory service encountered an unknown failure".		
2022-02 Servicing Stack Update for Windows Embedded Standard 7 for x86-based Systems.	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.	KB5010451	N/A
2022-02 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 KB5009610 (released January 11, 2022) and update KB5010798 (released January 17, 2022).	KB5010404	N/A

	Additionally, this update also addresses the following issues: Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. Addresses SHA1 deprecation by removing specific SHA1-signed security and non-security fixes and resigned those fixes with SHA2 in this release. Addresses an issue in which a Lightweight Directory Access Protocol (LDAP) modify operation that contains the SamAccountName together with the UserAccountControl attributes fails with "Error: 0x20EF The directory service encountered an unknown failure." Addresses an issue in which Windows Server 2008 R2 domain controllers (DCs) fail to process NTLM pass-through authentication. Adds an audit event on Active Directory domain controllers that identifies clients that are not RFC-4456 compliant. For more information, see KB5005408—Smart card authentication might cause print and scan failures.		
2022-02 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems.	This security update includes quality improvements. Key changes include: Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. Addresses SHA1 deprecation by removing specific SHA1-signed security and non-security fixes and resigned those fixes with SHA2 in this release. Addresses an issue in which Windows Server 2008 R2 domain controllers (DCs) fail to process NTLM pass-through authentication. Addresses an issue in which a Lightweight Directory Access Protocol (LDAP) modify operation that contains the SamAccountName together with the UserAccountControl attributes fails with "Error: 0x20EF The directory service encountered an unknown failure."	KB5010422	N/A

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

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

Microsoft® & Third-Party Patches

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

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

Patch Name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.98	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	N/A
2022-02 Cumulative Update for Windows Server 2016 for x64-based Systems.	This security update includes quality improvements. Key changes include: Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. Updates the phone number for Windows Activation for locales that have the wrong phone number. Addresses an issue that causes Windows to stop working and generates the error, "IRQL_NOT_LESS_OR_EQUAL". Addresses an issue that causes the improper cleanup of Dynamic Data Exchange (DDE) objects. This prevents session teardown and causes a session to stop responding. Addresses an access violation in IKEEXT.dll that occurs on Always On VPN (AOVPN) and DirectAccess servers. The exception code is 0xC000005. Addresses an issue that affects Administrative Template settings you configure using a Group Policy Object (GPO). When you change the value of the policy setting to NOT CONFIGURED, the system fails to remove the previous setting.	KB5010359	N/A

	This issue is most noticeable for roaming user profiles. Addresses a memory leak that occurs when you call WinVerifyTrust(). This issue occurs if verification fails for the first signature of a file that has multiple signatures. Addresses a known issue that affects versions of Windows Server that are in use as a Key Management Services (KMS) host. Client devices running Windows 10 Enterprise LTSC 2016 might not activate. This issue only occurs when using a new Customer Support Volume License Key (CSVLK) and after installing updates released April 22, 2021 or later. Adds an audit event to Active Directory domain controllers that identifies clients that are not compliant with RFC 4456. For more information, see KB5005408: Smart card authentication might cause print and scan failures. Addresses an issue that might cause Kerberos.dll to stop working within the Local Security Authority Subsystem Service (LSASS). This occurs when LSASS processes simultaneous Service for User (S4U) user-to-user (U2U) requests for the same client user. Addresses an issue that causes a Lightweight Directory Access Protocol (LDAP) modify operation to fail if the operation contains the SamAccountName and UserAccountControl attributes. The error message is, "Error: 0x20EF. The directory service encountered ar unknown failure".		
2022-02 Cumulative Update for Windows 10 Version 1607 for x64-based Systems.	This security update includes quality improvements. Key changes include: Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. Updates the phone number for Windows Activation for locales that have the wrong phone number. Addresses an issue that causes Windows to stop working and generates the error, "IRQL_NOT_LESS_OR_EQUAL". Addresses an issue that causes the improper cleanup of Dynamic Data Exchange (DDE) objects. This prevents	KB5010359	N/A

	session teardown and causes a session to stop responding. Addresses an access violation in IKEEXT.dll that occurs on Always On VPN (AOVPN) and DirectAccess servers. The exception code is 0xC000005. Addresses an issue that affects Administrative Template settings you configure using a Group Policy Object (GPO). When you change the value of the policy setting to NOT CONFIGURED, the system fails to remove the previous setting. This issue is most noticeable for roaming user profiles. Addresses a memory leak that occurs when you call WinVerifyTrust(). This issue occurs if verification fails for the first signature of a file that has multiple signatures. Addresses a known issue that affects versions of Windows Server that are in use as a Key Management Services (KMS) host. Client devices running Windows 10 Enterprise LTSC 2016 might not activate. This issue only occurs when using a new Customer Support Volume License Key (CSVLK) and after installing updates released April 22, 2021 or later. Adds an audit event to Active Directory domain controllers that identifies clients that are not compliant with RFC 4456. For more information, see KB5005408: Smart card authentication might cause print and scan failures. Addresses an issue that might cause Kerberos.dll to stop working within the Local Security Authority Subsystem Service (LSASS). This occurs when LSASS processes simultaneous Service for User (S4U) user-to-user (U2U) requests for the same client user. Addresses an issue that causes a Lightweight Directory Access Protocol (LDAP) modify operation to fail if the operation contains the SamAccountName and UserAccountControl attributes. The error message is, "Error: 0x20EF. The directory service encountered an unknown failure".		

Windows Malicious Software Removal Tool - v5.98	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	N/A
2022-02 Servicing Stack Update for Windows Embedded Standard 7 for x86-based Systems.	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.	KB5010451	N/A
2022-02 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 KB5009610 (released January 11, 2022) and update KB5010798 (released January 17, 2022). Additionally, this update also addresses the following issues: Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. Addresses SHA1 deprecation by removing specific SHA1-signed security and non-security fixes and resigned those fixes with SHA2 in this release. Addresses an issue in which a Lightweight Directory Access Protocol (LDAP) modify operation that contains the SamAccountName together with the UserAccountControl attributes fails with "Error: 0x20EF The directory service encountered an unknown failure." Addresses an issue in which Windows Server 2008 R2 domain controllers (DCs) fail to process NTLM pass-through authentication. Adds an audit event on Active Directory domain controllers that identifies clients that are not RFC-4456 compliant. For more information, see KB5005408—Smart card authentication might cause print and scan failures.	KB5010404	N/A
2022-02 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems.	This security update includes quality improvements. Key changes include: Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. Addresses SHA1 deprecation by removing specific SHA1-signed security and non-security fixes and resigned those fixes with SHA2 in this release.	KB5010422	N/A

	Addresses an issue in which Windows Server 2008 R2 domain controllers (DCs) fail to process NTLM pass-through authentication. Addresses an issue in which a Lightweight Directory Access Protocol (LDAP) modify operation that contains the SamAccountName together with the UserAccountControl attributes fails with "Error: 0x20EF The directory service encountered an unknown failure."		
2022-02 Security Only Quality Update for Windows Server 2008 for x86-based Systems.	This security update includes quality improvements. Key changes include: Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. Addresses an issue in which a Lightweight Directory Access Protocol (LDAP) modify operation that contains the SamAccountName together with the UserAccountControl attributes fails with "Error: 0x20EF The directory service encountered an unknown failure."	KB5010403	N/A
2022-02 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 KB5009627 (released January 11, 2022) and update KB5010799 (released January 17, 2022). Additionally, this update also addresses the following issues: Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. Adds an audit event on Active Directory domain controllers that identifies clients that are not RFC-4456 compliant. For more information, see KB5005408—Smart card authentication might cause print and scan failures. Addresses an issue in which a Lightweight Directory Access Protocol (LDAP) modify operation that contains the SamAccountName together with the UserAccountControl attributes fails with "Error: 0x20EF The directory service encountered an unknown failure."	KB5010384	N/A

2022-02 Servicing Stack Update for Windows Server 2008 for x86-based Systems.	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) make sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.	KB5010452	N/A

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

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

Microsoft® & Third-Party Patches

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

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

Patch Name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool - v5.98	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers.	KB890830	N/A
2022-02 Servicing Stack Update for Windows Embedded Standard 7 for x86-based Systems.	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.	KB5010451	N/A
2022-02 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 KB5009610 (released January 11, 2022) and update KB5010798 (released January 17, 2022). Additionally, this update also addresses the following issues: Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. Addresses SHA1 deprecation by removing specific SHA1-signed security and non-security fixes and resigned those fixes with SHA2 in this release. Addresses an issue in which a Lightweight Directory Access Protocol (LDAP) modify operation that contains the SamAccountName together with the UserAccountControl attributes fails with	KB5010404	N/A

	"Error: 0x20EF The directory service encountered an unknown failure." Addresses an issue in which Windows Server 2008 R2 domain controllers (DCs) fail to process NTLM pass-through authentication. Adds an audit event on Active Directory domain controllers that identifies clients that are not RFC-4456 compliant. For more information, see KB5005408—Smart card authentication might cause print and scan failures.		
2022-02 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems.	This security update includes quality improvements. Key changes include: Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. Addresses SHA1 deprecation by removing specific SHA1-signed security and non-security fixes and resigned those fixes with SHA2 in this release. Addresses an issue in which Windows Server 2008 R2 domain controllers (DCs) fail to process NTLM pass-through authentication. Addresses an issue in which a Lightweight Directory Access Protocol (LDAP) modify operation that contains the SamAccountName together with the UserAccountControl attributes fails with "Error: 0x20EF The directory service encountered an unknown failure."	KB5010422	N/A

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

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

Microsoft® & Third-Party Patches

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

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

Patch Name	Description	Patch ID	Notes
2022-02 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 KB5009610 (released January 11, 2022) and update KB5010798 (released January 17, 2022). Additionally, this update also addresses the following issues: Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. Addresses SHA1 deprecation by removing specific SHA1-signed security and non-security fixes and resigned those fixes with SHA2 in this release. Addresses an issue in which a Lightweight Directory Access Protocol (LDAP) modify operation that contains the SamAccountName together with the UserAccountControl attributes fails with "Error: 0x20EF The directory service encountered an unknown failure." Addresses an issue in which Windows Server 2008 R2 domain controllers (DCs) fail to process NTLM pass-through authentication. Adds an audit event on Active Directory domain controllers that	KB5010404	N/A

	identifies clients that are not RFC-4456 compliant. For more information, see KB5005408—Smart card authentication might cause print and scan failures.		
2022-02 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems.	This security update includes quality improvements. Key changes include: Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. Addresses SHA1 deprecation by removing specific SHA1-signed security and non-security fixes and resigned those fixes with SHA2 in this release. Addresses an issue in which Windows Server 2008 R2 domain controllers (DCs) fail to process NTLM pass-through authentication. Addresses an issue in which a Lightweight Directory Access Protocol (LDAP) modify operation that contains the SamAccountName together with the UserAccountControl attributes fails with "Error: 0x20EF The directory service encountered an unknown failure."	KB5010422	N/A
2022-02 Servicing Stack Update for Windows Embedded Standard 7 for x86-based Systems.	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.	KB5010451	N/A

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

Date of Critical or Security Patches: February 2022

Abstract: Critical or Security Patches – February 2022

Microsoft® & Third-Party Patches

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

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

Patch Name	Description	Patch ID	Notes
2022-02 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 KB5009610 (released January 11, 2022) and update KB5010798 (released January 17, 2022). Additionally, this update also addresses the following issues: Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. Addresses SHA1 deprecation by removing specific SHA1-signed security and non-security fixes and resigned those fixes with SHA2 in this release. Addresses an issue in which a Lightweight Directory Access Protocol (LDAP) modify operation that contains the SamAccountName together with the UserAccountControl attributes fails with "Error:	KB5010404	None

	0x20EF The directory service encountered an unknown failure." Addresses an issue in which Windows Server 2008 R2 domain controllers (DCs) fail to process NTLM pass-through authentication. Adds an audit event on Active Directory domain controllers that identifies clients that are not RFC-4456 compliant. For more information, see KB5005408—Smart card authentication might cause print and scan failures.		
2022-02 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems.	This security update includes quality improvements. Key changes include: Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. Addresses SHA1 deprecation by removing specific SHA1-signed security and non-security fixes and resigned those fixes with SHA2 in this release. Addresses an issue in which Windows Server 2008 R2 domain controllers (DCs) fail to process NTLM pass-through authentication. Addresses an issue in which a Lightweight Directory Access Protocol (LDAP) modify operation that contains the SamAccountName together with the UserAccountControl attributes fails with "Error: 0x20EF The directory service	KB5010422	None

	encountered an unknown failure.”		
2022-02 Servicing Stack Update for Windows Embedded Standard 7 for x86-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.	KB5010451	None
Windows Malicious Software Removal Tool x64 - v5.98	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	None

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

Date of Critical or Security Patches: February 2022

Abstract: Critical or Security Patches – February 2022

Microsoft® & Third-Party Patches

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

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

Patch Name	Description	Patch ID	Notes
2022-02 Cumulative Update for Windows 10 Version 1809 for x64-based Systems	A security issue has been iden tified 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.	KB5010351	None
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 iden tified 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	None

2021-08 Servicing Stack Update for Windows 10 Version 1809 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.	KB5005112	None
Security Update for SQL Server 2016 Service Pack 2 GDR	A remote code execution vulnerability exists in Microsoft SQL Server when it incorrectly handles processing of internal functions. An attacker who successfully exploited this vulnerability could execute code in the context of the SQL Server Database Engine service account. To exploit the vulnerability, an authenticated attacker would need to submit a specially crafted query to an affected SQL server. The security update addresses the vulnerability by modifying how the Microsoft SQL Server Database Engine handles the processing of functions.	KB4505220	None
Security Update for Windows 10 Version 1809 for x64-based Systems	A security issue has been iden tified 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.	KB4535680	None

Windows Malicious Software Removal Tool x64 - v5.98	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	None

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

Date of Critical or Security Patches: February 2022

Abstract: Critical or Security Patches – February 2022

Microsoft® & Third-Party Patches

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

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

Patch Name	Description	Patch ID	Notes
2022-02 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5010419)	This security update includes improvements and fixes that were a part of update KB5009624 (released January 11, 2022) and update KB5010794 (released January 17, 2022). Additionally, this update also addresses the following issues: • Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. • Addresses an issue in which virtual machines (VMs) on a Windows server that has Unified Extensible Firmware Interface (UEFI) enabled fail to start after installing the January 11, 2022 Windows update. • Addresses an issue in which Windows stops running with an	KB5010419	None

	IRQL_NOT_LESS_OR_EQUAL error. • Addresses an issue in which a Lightweight Directory Access Protocol (LDAP) modify operation that contains the SamAccountName together with the UserAccountControl attributes fails with "Error: 0x20EF The directory service encountered an unknown failure." Adds an audit event on Active Directory domain controllers that identifies clients that are not RFC-4456 compliant. For more information, see KB5005408—Smart card authentication might cause print and scan failures.		
2022-02 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5010395)	This security update includes quality improvements. Key changes include: • Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. • Addresses an issue in which virtual machines (VMs) on a Windows server that has Unified Extensible Firmware Interface (UEFI) enabled fail to start after installing the January 11, 2022 Windows update. • Addresses an issue in which Windows stops running with an IRQL_NOT_LESS_OR_EQUAL error.	KB5010395	None

	Addresses an issue in which a Lightweight Directory Access Protocol (LDAP) modify operation that contains the SamAccountName together with the UserAccountControl attributes fails with "Error: 0x20EF The directory service encountered an unknown failure."		
2022-02 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 KB5009610 (released January 11, 2022) and update KB5010798 (released January 17, 2022). Additionally, this update also addresses the following issues: Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. Addresses SHA1 deprecation by removing specific SHA1-signed security and non-security fixes and resigned those fixes with SHA2 in this release. Addresses an issue in which a Lightweight Directory Access Protocol (LDAP) modify operation that contains the SamAccountName together with the UserAccountControl attributes fails with "Error: 0x20EF The directory service encountered an unknown failure." Addresses an issue in which Windows Server 2008 R2 domain controllers (DCs) fail	KB5010404	None

	to process NTLM pass-through authentication. Adds an audit event on Active Directory domain controllers that identifies clients that are not RFC-4456 compliant. For more information, see KB5005408—Smart card authentication might cause print and scan failures.		
2022-02 Security Only Quality Update for Windows Embedded Standard 7 for x86-based Systems.	This security update includes quality improvements. Key changes include: Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. Addresses SHA1 deprecation by removing specific SHA1-signed security and non-security fixes and resigned those fixes with SHA2 in this release. Addresses an issue in which Windows Server 2008 R2 domain controllers (DCs) fail to process NTLM pass-through authentication. Addresses an issue in which a Lightweight Directory Access Protocol (LDAP) modify operation that contains the SamAccountName together with the UserAccountControl attributes fails with "Error: 0x20EF The directory service encountered an unknown failure."	KB5010422	None
2022-02 Servicing Stack Update for Windows Embedded	Install this update to resolve issues in Windows. For a complete listing of the issues that	KB5010451	None

Standard 7 for x86-based Systems	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.		
Windows Malicious Software Removal Tool x64 - v5.98	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	None

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

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

Microsoft® & Third-Party Patches

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

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

Patch Name	Description	Patch ID	Notes
2022-02 Security Monthly Quality Rollup 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.	KB5010404	N/A
2022-02 Servicing Stack Update for Windows Embedded Standard 7 for x86-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.	KB5010451	N/A
2022-02 Security and Quality Rollup for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7,	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	KB5010581	N/A

4.7.1, 4.7.2, 4.8 for Windows Server 2008 R2 for x64	article for more information. After you install this item, you may have to restart your computer.		
2022-02 Security Only Quality Update for Windows Embedded Standard 7 for x64-based Systems	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.	KB5010422	N/A

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

Date of Critical or Security Patches: February 2022
Abstract: Critical or Security Patches: February 2022

Microsoft® & Third-Party Patches

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

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

Patch Name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.98	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers that are running any of the following operating systems: • Windows 10 • Windows Server 2019 • Windows Server 2016 • Windows 8.1 • Windows Server 2012 R2 • Windows Server 2012 • Windows 7 • Windows Server 2008 R2 for x64-based Systems	KB890830	None
2022-02 Cumulative Update for x64-based Systems	• Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. • Updates security for your Windows operating system.	KB5010359	None

2022-02 Security Only Update for x64-based Systems	This security update includes improvements and fixes that were a part of update KB5009624 (released January 11, 2022) and update KB5010794 (released January 17, 2022). Additionally, this update also addresses the following issues: • Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. • Addresses an issue in which virtual machines (VMs) on a Windows server that has Unified Extensible Firmware Interface (UEFI) enabled fail to start after installing the January 11, 2022 Windows update. • Addresses an issue in which Windows stops running with an IRQL_NOT_LESS_OR_EQUAL error. • Addresses an issue in which a Lightweight Directory Access Protocol (LDAP) modify operation that contains the SamAccountName together with the UserAccountControl attributes fails with "Error: 0x20EF The directory service encountered an unknown failure."	KB5010419	None

BD Product Name: **BD Pyxis™ Supply**

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

Microsoft® & Third-Party Patches

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

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

Patch Name	Description	Patch ID	Notes
2022-02 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5010395)	This security update includes quality improvements. Key changes include: • Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. • Addresses an issue in which virtual machines (VMs) on a Windows server that has Unified Extensible Firmware Interface (UEFI) enabled fail to start after installing the January 11, 2022 Windows update. • Addresses an issue in which Windows stops running with an IRQL_NOT_LESS_OR_EQUAL error. • Addresses an issue in which a Lightweight Directory Access Protocol (LDAP) modify operation that contains the SamAccountName together with the UserAccountControl attributes fails with	KB5010395	None

	"Error: 0x20EF The directory service encountered an unknown failure."		
2022-02 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5010419)	This security update includes improvements and fixes that were a part of update KB5009624 (released January 11, 2022) and update KB5010794 (released January 17, 2022). Additionally, this update also addresses the following issues: • Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. • Addresses an issue in which virtual machines (VMs) on a Windows server that has Unified Extensible Firmware Interface (UEFI) enabled fail to start after installing the January 11, 2022 Windows update. • Addresses an issue in which Windows stops running with an IRQL_NOT_LESS_OR_EQUAL error. • Addresses an issue in which a Lightweight Directory Access Protocol (LDAP) modify operation that contains the SamAccountName together with the UserAccountControl attributes fails with "Error: 0x20EF The directory service encountered an unknown failure."	KB5010419	None

	• Adds an audit event on Active Directory domain controllers that identifies clients that are not RFC-4456 compliant. For more information, see KB5005408—Smart card authentication might cause print and scan failures.		
2022-02 Servicing Stack Update for Windows 7 for x86-based Systems (KB5010451)	Windows 7 and Windows Server 2008 R2 have reached the end of mainstream support and are now in extended security update (ESU) support.	KB5010451	None
2022-02 Security Monthly Quality Rollup for Windows 7 for x86-based Systems (KB5010404)	This security update includes improvements and fixes that were a part of update KB5009610 (released January 11, 2022) and update KB5010798 (released January 17, 2022). Additionally, this update also addresses the following issues: • Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. • Addresses SHA1 deprecation by removing specific SHA1-signed security and non-security fixes and resigned those fixes with SHA2 in this release. • Addresses an issue in which a Lightweight Directory Access Protocol (LDAP) modify operation that contains the SamAccountName together with the UserAccountControl attributes fails with	KB5010404	None

	"Error: 0x20EF The directory service encountered an unknown failure." • Addresses an issue in which Windows Server 2008 R2 domain controllers (DCs) fail to process NTLM pass-through authentication. • Adds an audit event on Active Directory domain controllers that identifies clients that are not RFC-4456 compliant. For more information, see KB5005408—Smart card authentication might cause print and scan failures.		
2022-02 Security Only Quality Update for Windows 7 for x86-based Systems (KB5010422)	This security update includes quality improvements. Key changes include: • Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. • Addresses SHA1 deprecation by removing specific SHA1-signed security and non-security fixes and resigned those fixes with SHA2 in this release. • Addresses an issue in which Windows Server 2008 R2 domain controllers (DCs) fail to process NTLM pass-through authentication. • Addresses an issue in which a Lightweight Directory Access Protocol (LDAP)	KB5010422	None

	modify operation that contains the SamAccountName together with the UserAccountControl attributes fails with "Error: 0x20EF The directory service encountered an unknown failure."		
2022-02 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5010359)	This security update includes quality improvements. Key changes include: • Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. • Updates the phone number for Windows Activation for locales that have the wrong phone number. • Addresses an issue that causes Windows to stop working and generates the error, "IRQL_NOT_LESS_OR_EQUAL". • Addresses an issue that causes the improper cleanup of Dynamic Data Exchange (DDE) objects. This prevents session teardown and causes a session to stop responding. • Addresses an access violation in IKEEXT.dll that occurs on Always On VPN (AOVPN) and DirectAccess servers. The exception code is 0xC000005. • Addresses an issue that affects Administrative	KB5010359	None

	Template settings you configure using a Group Policy Object (GPO). When you change the value of the policy setting to NOT CONFIGURED, the system fails to remove the previous setting. This issue is most noticeable for roaming user profiles. • Addresses a memory leak that occurs when you call WinVerifyTrust(). This issue occurs if verification fails for the first signature of a file that has multiple signatures. • Addresses a known issue that affects versions of Windows Server that are in use as a Key Management Services (KMS) host. Client devices running Windows 10 Enterprise LTSC 2016 might not activate. This issue only occurs when using a new Customer Support Volume License Key (CSVLK) and after installing updates released April 22, 2021 or later. • Adds an audit event to Active Directory domain controllers that identifies clients that are not compliant with RFC 4456. For more information, see KB5005408: Smart card authentication might cause print and scan failures.		

	• Addresses an issue that might cause Kerberos.dll to stop working within the Local Security Authority Subsystem Service (LSASS). This occurs when LSASS processes simultaneous Service for User (S4U) user-to-user (U2U) requests for the same client user. • Addresses an issue that causes a Lightweight Directory Access Protocol (LDAP) modify operation to fail if the operation contains the SamAccountName and UserAccountControl attributes. The error message is, "Error: 0x20EF. The directory service encountered an unknown failure".		
2022-02 Cumulative Update for Windows 10 Version 1809 for x86-based Systems (KB5010351)	This security update includes quality improvements. Key changes include: • Addresses an issue that causes a Lightweight Directory Access Protocol (LDAP) modify operation to fail if the operation contains the SamAccountName and UserAccountControl attributes. The error message is, "Error: 0x20EF. The directory service encountered an unknown failure". • Addresses a known issue that might prevent recent emails from appearing in	KB5010351	None

	search results in the Microsoft Outlook desktop app. This issue is related to emails that have been stored locally in a .pst or .ost files. It might affect POP and IMAP accounts, as well as accounts hosted on Microsoft Exchange and Microsoft 365. If the default search in the Microsoft Outlook app is set to server search, the issue will only affect the advanced search.		
Windows Malicious Software Removal Tool x64 - v5.98	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers. Microsoft releases the MSRT on a monthly cadence as part of Windows Update or as a standalone tool. Use this tool to find and remove specific prevalent threats and reverse the changes they have made.	KB890830	None

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

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

Microsoft® & Third-Party Patches

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

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

Patch Name	Description	Patch ID	Notes
2022-02 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.	KB5010419	None
2022-02 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.	KB5010395	None

2022-02 Security and Quality Rollup for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows Server 2012 R2 for x64	Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.	KB5010583	None
2022-02 Security and Quality Rollup for .NET Framework 4.8 for Windows Server 2012 R2 for x64	Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.	KB5010462	None
Windows Malicious Software Removal Tool x64 - v5.98	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	KB890830	None

2022-02 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.	KB5010359	None

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

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

Microsoft® & Third-Party Patches

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

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

Patch Name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers that are running any of the following operating systems: 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 OS: Windows Server 2016, Windows Server 2008, Windows Server 2012	KB890830	N/A
2022-02 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.	KB5010395	N/A

2022-02 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.	KB5010419	N/A
2022-02 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.	KB5010359	N/A

BD Product Name: **BD Pyxis® PARx**

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

Microsoft® & Third-Party Patches

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

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

Patch Name	Description	Patch ID	Notes
2022-02 Cumulative Update for Windows 10 Version 1607 for x64-based Systems (KB5010359)	This security update includes quality improvements. Key changes include: Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. Updates the phone number for Windows Activation for locales that have the wrong phone number. Addresses an issue that causes Windows to stop working and generates the error, "IRQL_NOT_LESS_OR_EQUAL". Addresses an issue that causes the improper cleanup of Dynamic Data Exchange (DDE) objects. This prevents session teardown and causes a session to stop responding. Addresses an access violation in IKEEXT.dll that occurs on Always On VPN (AOVPN) and DirectAccess	KB5010359	None

	servers. The exception code is 0xC000005. Addresses an issue that affects Administrative Template settings you configure using a Group Policy Object (GPO). When you change the value of the policy setting to NOT CONFIGURED, the system fails to remove the previous setting. This issue is most noticeable for roaming user profiles. Addresses a memory leak that occurs when you call WinVerifyTrust(). This issue occurs if verification fails for the first signature of a file that has multiple signatures. Addresses a known issue that affects versions of Windows Server that are in use as a Key Management Services (KMS) host. Client devices running Windows 10 Enterprise LTSC 2016 might not activate. This issue only occurs when using a new Customer Support Volume License Key (CSVLK) and after installing updates released April 22, 2021 or later. Adds an audit event to Active Directory domain controllers that identifies clients that are not compliant with RFC 4456. For more information, see KB5005408: Smart card authentication might cause print and scan failures. Addresses an issue that might cause Kerberos.dll to stop working within the Local Security Authority Subsystem Service (LSASS). This occurs when LSASS processes simultaneous Service for User (S4U) user-to-user (U2U) requests for the same client user.		

	Addresses an issue that causes a Lightweight Directory Access Protocol (LDAP) modify operation to fail if the operation contains the SamAccountName and UserAccountControl attributes. The error message is, "Error: 0x20EF. The directory service encountered an unknown failure".		

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

Microsoft® & Third-Party Patches

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

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

Patch Name	Description	Patch ID	Notes
Windows Malicious Software Removal Tool x64 - v5.85	The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers that are running any of the following operating systems: Windows 10 Windows Server 2019 Windows Server 2016 Windows 8.1 Windows Server 2012 R2 Windows Server 2012 Windows 7 Windows Server 2008 R2 for x64-based Systems	KB890830	N/A
2022-01 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (KB5009610)	Improvements and fixes This security update includes improvements and fixes that were a part of update KB5008244 (released December 14, 2021) and addresses the following issues: • This update contains miscellaneous security improvements to internal OS functionality. No specific issues are documented for this release.	KB5009610	N/A

2022-02 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB5010395)	Improvements and fixes This security update includes quality improvements. Key changes include: • Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. • Addresses an issue in which virtual machines (VMs) on a Windows server that has Unified Extensible Firmware Interface (UEFI) enabled fail to start after installing the January 11, 2022 Windows update. • Addresses an issue in which Windows stops running with an IRQL_NOT_LESS_OR_EQUAL error. • Addresses an issue in which a Lightweight Directory Access Protocol (LDAP) modify operation that contains the **SamAccountName** together with the **UserAccountControl** attributes fails with "Error: 0x20EF The directory service encountered an unknown failure."	KB5010395	N/A
2022-02 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5010419)	Improvements and fixes This security update includes improvements and fixes that were a part of update KB5009624 (released January 11, 2022) and update KB5010794 (released January 17, 2022). Additionally, this update also addresses the following issues: • Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan.	KB5010419	N/A

	• Addresses an issue in which virtual machines (VMs) on a Windows server that has Unified Extensible Firmware Interface (UEFI) enabled fail to start after installing the January 11, 2022 Windows update. • Addresses an issue in which Windows stops running with an IRQL_NOT_LESS_OR_EQUAL error. • Addresses an issue in which a Lightweight Directory Access Protocol (LDAP) modify operation that contains the **SamAccountName** together with the **UserAccountControl** attributes fails with "Error: 0x20EF The directory service encountered an unknown failure."		
2022-02 Cumulative Update for Windows Server 2016 for x64-based Systems (KB5010359)	Improvements and fixes This security update includes quality improvements. Key changes include: • Updates daylight savings time to start in February 2022 instead of March 2022 in Jordan. • Updates the phone number for Windows Activation for locales that have the wrong phone number. • Addresses an issue that causes Windows to stop working and generates the error, "IRQL_NOT_LESS_OR_EQUAL". • Addresses an issue that causes the improper cleanup of Dynamic Data Exchange (DDE) objects. This prevents	KB5010359	N/A

	session teardown and causes a session to stop responding. • Addresses an access violation in **IKEEXT.dll** that occurs on Always On VPN (AOVPN) and DirectAccess servers. The exception code is 0xC000005.		