Security Patches for Mindray Products Running on Windows OS (Nov, 2021)

CONTENT

To Whom It May Concern,

Below content is only for your information.

Introduction:

We have reviewed the applicability to Mindray products of the Microsoft Windows security patches released in Nov, 2021. The following CVEs have been evaluated:

CVE Identifiers

- CVE-2021-43209 3D Viewer Remote Code Execution Vulnerability
- CVE-2021-43208 3D Viewer Remote Code Execution Vulnerability
- CVE-2021-42323 Azure RTOS Information Disclosure Vulnerability
- CVE-2021-42322 Visual Studio Code Elevation of Privilege Vulnerability
- CVE-2021-42321 Microsoft Exchange Server Remote Code Execution Vulnerability
- CVE-2021-42319 Visual Studio Elevation of Privilege Vulnerability
- CVE-2021-42316 Microsoft Dynamics 365 (on-premises) Remote Code Execution Vulnerability
- CVE-2021-42307 Microsoft Edge (Chromium-based) Information Disclosure Vulnerability
- CVE-2021-42305 Microsoft Exchange Server Spoofing Vulnerability
- CVE-2021-42304 Azure RTOS Elevation of Privilege Vulnerability
- CVE-2021-42303 Azure RTOS Elevation of Privilege Vulnerability
- CVE-2021-42302 Azure RTOS Elevation of Privilege Vulnerability
- CVE-2021-42301 Azure RTOS Information Disclosure Vulnerability
- CVE-2021-42300 Azure Sphere Tampering Vulnerability
- CVE-2021-42299 Microsoft Surface Pro 3 Security Feature Bypass Vulnerability
- CVE-2021-42298 Microsoft Defender Remote Code Execution Vulnerability
- CVE-2021-42296 Microsoft Word Remote Code Execution Vulnerability
- CVE-2021-42292 Microsoft Excel Security Feature Bypass Vulnerability
- CVE-2021-42291 Active Directory Domain Services Elevation of Privilege Vulnerability
- CVE-2021-42287 Active Directory Domain Services Elevation of Privilege Vulnerability
- CVE-2021-42286 Windows Core Shell SI Host Extension Framework for Composable Shell Elevation of Privilege Vulnerability
- CVE-2021-42285 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2021-42284 Windows Hyper-V Denial of Service Vulnerability
- CVE-2021-42283 NTFS Elevation of Privilege Vulnerability
- CVE-2021-42282 Active Directory Domain Services Elevation of Privilege Vulnerability
- CVE-2021-42280 Windows Feedback Hub Elevation of Privilege Vulnerability
- CVE-2021-42279 Chakra Scripting Engine Memory Corruption Vulnerability
- CVE-2021-42278 Active Directory Domain Services Elevation of Privilege Vulnerability
- CVE-2021-42277 Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
- CVE-2021-42276 Microsoft Windows Media Foundation Remote Code Execution Vulnerability
- CVE-2021-42275 Microsoft COM for Windows Remote Code Execution Vulnerability

- CVE-2021-42274 Windows Hyper-V Discrete Device Assignment (DDA) Denial of Service Vulnerability
- CVE-2021-41379 Windows Installer Elevation of Privilege Vulnerability
- CVE-2021-41378 Windows NTFS Remote Code Execution Vulnerability
- CVE-2021-41377 Windows Fast FAT File System Driver Elevation of Privilege Vulnerability
- CVE-2021-41376 Azure Sphere Information Disclosure Vulnerability
- CVE-2021-41375 Azure Sphere Information Disclosure Vulnerability
- CVE-2021-41374 Azure Sphere Information Disclosure Vulnerability
- CVE-2021-41373 FSLogix Information Disclosure Vulnerability
- CVE-2021-41372 Power BI Report Server Spoofing Vulnerability
- CVE-2021-41371 Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability
- CVE-2021-41370 NTFS Elevation of Privilege Vulnerability
- CVE-2021-41368 Microsoft Access Remote Code Execution Vulnerability
- CVE-2021-41367 NTFS Elevation of Privilege Vulnerability
- CVE-2021-41366 Credential Security Support Provider Protocol (CredSSP) Elevation of Privilege Vulnerability
- CVE-2021-41363 Intune Management Extension Security Feature Bypass Vulnerability
- CVE-2021-41356 Windows Denial of Service Vulnerability
- CVE-2021-41355 .NET Core and Visual Studio Information Disclosure Vulnerability
- CVE-2021-41354 Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability
- CVE-2021-41353 Microsoft Dynamics 365 (on-premises) Spoofing Vulnerability
- CVE-2021-41351 Microsoft Edge (Chrome based) Spoofing on IE Mode
- CVE-2021-41349 Microsoft Exchange Server Spoofing Vulnerability
- CVE-2021-41344 Microsoft SharePoint Server Remote Code Execution Vulnerability
- CVE-2021-40487 Microsoft SharePoint Server Remote Code Execution Vulnerability
- CVE-2021-40485 Microsoft Excel Remote Code Execution Vulnerability
- CVE-2021-40457 Microsoft Dynamics 365 Customer Engagement Cross-Site Scripting Vulnerability
- CVE-2021-40442 Microsoft Excel Remote Code Execution Vulnerability
- CVE-2021-38666 Remote Desktop Client Remote Code Execution Vulnerability
- CVE-2021-38665 Remote Desktop Protocol Client Information Disclosure Vulnerability
- CVE-2021-38631 Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability
- CVE-2021-38003 Chromium: CVE-2021-38003 Inappropriate implementation in V8
- CVE-2021-38002 Chromium: CVE-2021-38002 Use after free in Web Transport
- CVE-2021-38001 Chromium: CVE-2021-38001 Type Confusion in V8
- CVE-2021-38000 Chromium: CVE-2021-38000 Insufficient validation of untrusted input in Intents
- CVE-2021-37999 Chromium: CVE-2021-37999 Insufficient data validation in New Tab Page
- CVE-2021-37998 Chromium: CVE-2021-37998 Use after free in Garbage Collection
- CVE-2021-37997 Chromium: CVE-2021-37997 Use after free in Sign-In
- CVE-2021-37996 Chromium: CVE-2021-37996 Insufficient validation of untrusted input in Downloads
- CVE-2021-37995 Chromium: CVE-2021-37995 Inappropriate implementation in WebApp Installer

- CVE-2021-37994 Chromium: CVE-2021-37994 Inappropriate implementation in iFrame Sandbox
- CVE-2021-37993 Chromium: CVE-2021-37993 Use after free in PDF Accessibility
- CVE-2021-37992 Chromium: CVE-2021-37992 Out of bounds read in WebAudio
- CVE-2021-37991 Chromium: CVE-2021-37991 Race in V8
- CVE-2021-37990 Chromium: CVE-2021-37990 Inappropriate implementation in WebView
- CVE-2021-37989 Chromium: CVE-2021-37989 Inappropriate implementation in Blink
- CVE-2021-37988 Chromium: CVE-2021-37988 Use after free in Profiles
- CVE-2021-37987 Chromium: CVE-2021-37987 Use after free in Network APIs
- CVE-2021-37986 Chromium: CVE-2021-37986 Heap buffer overflow in Settings
- CVE-2021-37985 Chromium: CVE-2021-37985 Use after free in V8
- CVE-2021-37984 Chromium: CVE-2021-37984 Heap buffer overflow in PDFium
- CVE-2021-37983 Chromium: CVE-2021-37983 Use after free in Dev Tools
- CVE-2021-37982 Chromium: CVE-2021-37982 Use after free in Incognito
- CVE-2021-37981 Chromium: CVE-2021-37981 Heap buffer overflow in Skia
- CVE-2021-3711 OpenSSL: CVE-2021-3711 SM2 Decryption Buffer Overflow
- CVE-2021-36957 Windows Desktop Bridge Elevation of Privilege Vulnerability
- CVE-2021-26444 Azure RTOS Information Disclosure Vulnerability
- CVE-2021-26443 Microsoft Virtual Machine Bus (VMBus) Remote Code Execution Vulnerability
- CVE-2021-26414 Windows DCOM Server Security Feature Bypass

For more details, please refer to the Microsoft website: https://portal.msrc.microsoft.com/en-us/security-guidance.

Impacted Mindray Products:

The following table lists the impacted device and those hotfixes determined to be applicable to each device:

OS	Hotfix	Product	Download website	Pre-installed patch
Windows 10 Professional SP1 64bit 1809	KB5007206	BeneVision CMS eGateway BeneVision CMS Viewer Hypervisor X CMS	windows10.0-kb5007206-x64_f8ccc7d4574581576e74d86ccacc7fbf47d050f6.msu	KB4587735 KB5003243 KB5005112
Windows Server 2019	KB5007206	BeneVision CMS eGateway Hypervisor X CMS MLDAP Server BeneVision Mobile Server	windows10.0-kb5007206-x64_f8ccc7d4574581576e74d86ccacc7fbf47d050f6.msu	KB4587735 KB5003243 KB5005112
Windows 10 Version 1607 for 32-bit Systems	KB5007192	BeneVision CMS Viewer BeneVision CMS Hypervisor X CMS	windows10.0-kb5007192-x86_f727630bb86d3eeca455f6f13ef4bb214f962192.msu	KB4132216 KB4498947
Windows 10 Version 1607 for	KB5007192	BeneVision CMS eGateway	windows10.0-kb5007192-x64_1eb621234dd4a597a	KB4132216 KB4498947

x64-based Systems Windows Server 2012 R2		BeneVision CMS Viewer MLDAP Server Hypervisor X CMS	97769935f46fc868c5800d9.msu	
	KB5007255	BeneVision CMS eGateway	windows8.1-kb5007255-x64_c877068c3c0fbff9ba5d2995a8532fbb70b2716f.msu	
Windows Server 2016	KB5007247	BeneVision CMS Viewer BeneVision Mobile Server MLDAP Server	windows8.1-kb5007247-x64_7536d20ab5c66ee4156f408044a6c65482352acf.msu	
Windows Server 2016	KB5007192	BeneVision CMS eGateway MLDAP Server BeneVision Mobile Server	windows10.0-kb5007192-x64_1eb621234dd4a597a97769935f46fc868c5800d9.msu	KB4132216 KB4498947

Conclusion and Recommendation:

We have validated that the Mindray products of the latest version can perform to specification with the applicable patches applied to the OS. It is recommended that the applicable patches defined in the table above should be installed on the affected Mindray products.

If you need information on how to obtain the approved patches or have any question, please feel free to contact Mindray regional service engineer or Mindray Service Department (email: *service@mindray.com*).

Thank you for your kind attention and cooperation.

Sincerely yours,

Mindray Service Department
Shenzhen Mindray Bio-Medical Electronics Co., Ltd.

Release Time：2021-12-17