Security Patches for Mindray Products Running on Windows OS (Oct, 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 Oct, 2021. The following CVEs have been evaluated:

CVE Identifiers

- CVE-2021-41363 Intune Management Extension Security Feature Bypass Vulnerability
- CVE-2021-41361 Active Directory Federation Server Spoofing Vulnerability
- CVE-2021-41357 Win32k Elevation of Privilege 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-2021-41352 SCOM Information Disclosure Vulnerability
- CVE-2021-41350 Microsoft Exchange Server Spoofing Vulnerability
- CVE-2021-41348 Microsoft Exchange Server Elevation of Privilege Vulnerability
- CVE-2021-41347 Windows AppX Deployment Service Elevation of Privilege Vulnerability
- CVE-2021-41346 Console Window Host Security Feature Bypass Vulnerability
- CVE-2021-41345 Storage Spaces Controller Elevation of Privilege Vulnerability
- CVE-2021-41344 Microsoft SharePoint Server Remote Code Execution Vulnerability
- CVE-2021-41343 Windows Fast FAT File System Driver Information Disclosure Vulnerability
- CVE-2021-41342 Windows MSHTML Platform Remote Code Execution Vulnerability
- CVE-2021-41340 Windows Graphics Component Remote Code Execution Vulnerability
- CVE-2021-41339 Microsoft DWM Core Library Elevation of Privilege Vulnerability
- CVE-2021-41338 Windows AppContainer Firewall Rules Security Feature Bypass Vulnerability
- CVE-2021-41337 Active Directory Security Feature Bypass Vulnerability
- CVE-2021-41336 Windows Kernel Information Disclosure Vulnerability
- CVE-2021-41335 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2021-41334 Windows Desktop Bridge Elevation of Privilege Vulnerability
- CVE-2021-41332 Windows Print Spooler Information Disclosure Vulnerability
- CVE-2021-41331 Windows Media Audio Decoder Remote Code Execution Vulnerability
- CVE-2021-41330 Microsoft Windows Media Foundation Remote Code Execution Vulnerability
- CVE-2021-40489 Storage Spaces Controller Elevation of Privilege Vulnerability
- CVE-2021-40488 Storage Spaces Controller Elevation of Privilege Vulnerability
- CVE-2021-40487 Microsoft SharePoint Server Remote Code Execution Vulnerability
- CVE-2021-40486 Microsoft Word Remote Code Execution Vulnerability

- CVE-2021-40485 Microsoft Excel Remote Code Execution Vulnerability
- CVE-2021-40484 Microsoft SharePoint Server Spoofing Vulnerability
- CVE-2021-40483 Microsoft SharePoint Server Spoofing Vulnerability
- CVE-2021-40482 Microsoft SharePoint Server Information Disclosure Vulnerability
- CVE-2021-40481 Microsoft Office Visio Remote Code Execution Vulnerability
- CVE-2021-40480 Microsoft Office Visio Remote Code Execution Vulnerability
- CVE-2021-40479 Microsoft Excel Remote Code Execution Vulnerability
- CVE-2021-40478 Storage Spaces Controller Elevation of Privilege Vulnerability
- CVE-2021-40477 Windows Event Tracing Elevation of Privilege Vulnerability
- CVE-2021-40476 Windows AppContainer Elevation Of Privilege Vulnerability
- CVE-2021-40475 Windows Cloud Files Mini Filter Driver Information Disclosure Vulnerability
- CVE-2021-40475 Windows Cloud Files Mini Filter Driver Information Disclosure Vulnerability
- CVE-2021-40474 Microsoft Excel Remote Code Execution Vulnerability
- CVE-2021-40473 Microsoft Excel Remote Code Execution Vulnerability
- CVE-2021-40472 Microsoft Excel Information Disclosure Vulnerability
- CVE-2021-40471 Microsoft Excel Remote Code Execution Vulnerability
- CVE-2021-40470 DirectX Graphics Kernel Elevation of Privilege Vulnerability
- CVE-2021-40469 Windows DNS Server Remote Code Execution Vulnerability
- CVE-2021-40468 Windows Bind Filter Driver Information Disclosure Vulnerability
- CVE-2021-40467 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2021-40466 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2021-40465 Windows Text Shaping Remote Code Execution Vulnerability
- CVE-2021-40464 Windows Nearby Sharing Elevation of Privilege Vulnerability
- CVE-2021-40463 Windows NAT Denial of Service Vulnerability
- CVE-2021-40462 Windows Media Foundation Dolby Digital Atmos Decoders Remote Code Execution Vulnerability
- CVE-2021-40461 Windows Hyper-V Remote Code Execution Vulnerability
- CVE-2021-40460 Windows Remote Procedure Call Runtime Security Feature Bypass Vulnerability
- CVE-2021-40457 Microsoft Dynamics 365 Customer Engagement Cross-Site Scripting Vulnerability
- CVE-2021-40456 Windows AD FS Security Feature Bypass Vulnerability
- CVE-2021-40455 Windows Installer Spoofing Vulnerability
- CVE-2021-40454 Rich Text Edit Control Information Disclosure Vulnerability
- CVE-2021-40450 Win32k Elevation of Privilege Vulnerability
- CVE-2021-40449 Win32k Elevation of Privilege Vulnerability
- CVE-2021-40447 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2021-40444 Microsoft MSHTML Remote Code Execution Vulnerability
- CVE-2021-40443 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2021-38672 Windows Hyper-V Remote Code Execution Vulnerability
- CVE-2021-38671 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2021-38667 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2021-38663 Windows exFAT File System Information Disclosure Vulnerability

- CVE-2021-38662 Windows Fast FAT File System Driver Information Disclosure Vulnerability
- CVE-2021-38657 Microsoft Office Graphics Component Information Disclosure Vulnerability
- CVE-2021-38649 Open Management Infrastructure Elevation of Privilege Vulnerability
- CVE-2021-38648 Open Management Infrastructure Elevation of Privilege Vulnerability
- CVE-2021-38647 Open Management Infrastructure Remote Code Execution Vulnerability
- CVE-2021-38645 Open Management Infrastructure Elevation of Privilege Vulnerability
- CVE-2021-38639 Win32k Elevation of Privilege Vulnerability
- CVE-2021-38638 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
- CVE-2021-38637 Windows Storage Information Disclosure Vulnerability
- CVE-2021-38636 Windows Redirected Drive Buffering SubSystem Driver Information Disclosure Vulnerability
- CVE-2021-38635 Windows Redirected Drive Buffering SubSystem Driver Information Disclosure Vulnerability
- CVE-2021-38634 Microsoft Windows Update Client Elevation of Privilege Vulnerability
- CVE-2021-38633 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2021-38632 BitLocker Security Feature Bypass Vulnerability
- CVE-2021-38630 Windows Event Tracing Elevation of Privilege Vulnerability
- CVE-2021-38629 Windows Ancillary Function Driver for WinSock Information Disclosure Vulnerability
- CVE-2021-38628 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
- CVE-2021-38624 Windows Key Storage Provider Security Feature Bypass Vulnerability
- CVE-2021-37980 Chromium: CVE-2021-37980 Inappropriate implementation in Sandbox
- CVE-2021-37979 Chromium: CVE-2021-37979 Heap buffer overflow in WebRTC
- CVE-2021-37978 Chromium: CVE-2021-37978 Heap buffer overflow in Blink
- CVE-2021-37977 Chromium: CVE-2021-37977 Use after free in Garbage Collection
- CVE-2021-37976 Chromium: CVE-2021-37976 Information leak in core
- CVE-2021-37975 Chromium: CVE-2021-37975 Use after free in V8
- CVE-2021-37974 Chromium: CVE-2021-37974 Use after free in Safe Browsing
- CVE-2021-37973 Chromium: CVE-2021-37973 Use after free in Portals
- CVE-2021-37972 Chromium: CVE-2021-37972 Out of bounds read in libjpeg-turbo
- CVE-2021-37971 Chromium: CVE-2021-37971 Incorrect security UI in Web Browser UI
- CVE-2021-37970 Chromium: CVE-2021-37970 Use after free in File System API
- CVE-2021-37969 Chromium: CVE-2021-37969 Inappropriate implementation in Google Updater
- CVE-2021-37968 Chromium: CVE-2021-37968 Inappropriate implementation in Background Fetch API
- CVE-2021-37967 Chromium: CVE-2021-37967 Inappropriate implementation in Background Fetch API
- CVE-2021-37966 Chromium: CVE-2021-37966 Inappropriate implementation in Compositing
- CVE-2021-37965 Chromium: CVE-2021-37965 Inappropriate implementation in

Background Fetch API
- CVE-2021-37964 Chromium: CVE-2021-37964 Inappropriate implementation in ChromeOS Networking
- CVE-2021-37963 Chromium: CVE-2021-37963 Side-channel information leakage in DevTools
- CVE-2021-37962 Chromium: CVE-2021-37962 Use after free in Performance Manager
- CVE-2021-37961 Chromium: CVE-2021-37961 Use after free in Tab Strip
- CVE-2021-37960 Chromium: CVE-2021-37960 Inappropriate implementation in Blink graphics
- CVE-2021-37959 Chromium: CVE-2021-37959 Use after free in Task Manager
- CVE-2021-37958 Chromium: CVE-2021-37958 Inappropriate implementation in Navigation
- CVE-2021-37957 Chromium: CVE-2021-37957 Use after free in WebGPU
- CVE-2021-37956 Chromium: CVE-2021-37956 Use after free in Offline use
- CVE-2021-36975 Win32k Elevation of Privilege Vulnerability
- CVE-2021-36974 Windows SMB Elevation of Privilege Vulnerability
- CVE-2021-36973 Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability
- CVE-2021-36972 Windows SMB Information Disclosure Vulnerability
- CVE-2021-36970 Windows Print Spooler Spoofing Vulnerability
- CVE-2021-36969 Windows Redirected Drive Buffering SubSystem Driver Information Disclosure Vulnerability
- CVE-2021-36967 Windows WLAN AutoConfig Service Elevation of Privilege Vulnerability
- CVE-2021-36966 Windows Subsystem for Linux Elevation of Privilege Vulnerability
- CVE-2021-36965 Windows WLAN AutoConfig Service Remote Code Execution Vulnerability
- CVE-2021-36964 Windows Event Tracing Elevation of Privilege Vulnerability
- CVE-2021-36963 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2021-36962 Windows Installer Information Disclosure Vulnerability
- CVE-2021-36961 Windows Installer Denial of Service Vulnerability
- CVE-2021-36960 Windows SMB Information Disclosure Vulnerability
- CVE-2021-36959 Windows Authenticode Spoofing Vulnerability
- CVE-2021-36955 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2021-36954 Windows Bind Filter Driver Elevation of Privilege Vulnerability
- CVE-2021-36953 Windows TCP/IP Denial of Service Vulnerability
- CVE-2021-34506 Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability
- CVE-2021-3450 OpenSSL: CVE-2021-3450 CA certificate check bypass with X509_V_FLAG_X509_STRICT
- CVE-2021-3449 OpenSSL: CVE-2021-3449 NULL pointer deref in signature_algorithms processing
- CVE-2021-34475 Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
- CVE-2021-34453 Microsoft Exchange Server Denial of Service Vulnerability
- CVE-2021-33781 Azure AD Security Feature Bypass Vulnerability
- CVE-2021-30633 Chromium: CVE-2021-30633 Use after free in Indexed DB API

- CVE-2021-30631 Chromium: CVE-2021-30631 Type Confusion in Blink layout
- CVE-2021-30630 Chromium: CVE-2021-30630 Inappropriate implementation in Blink
- CVE-2021-30629 Chromium: CVE-2021-30629 Use after free in Permissions
- CVE-2021-30628 Chromium: CVE-2021-30628 Stack buffer overflow in ANGLE
- CVE-2021-30627 Chromium: CVE-2021-30627 Type Confusion in Blink layout
- CVE-2021-30626 Chromium: CVE-2021-30626 Out of bounds memory access in ANGLE
- CVE-2021-30625 Chromium: CVE-2021-30625 Use after free in Selection API
- CVE-2021-26442 Windows HTTP.sys Elevation of Privilege Vulnerability
- CVE-2021-26441 Storage Spaces Controller Elevation of Privilege Vulnerability
- CVE-2021-26435 Windows Scripting Engine Memory Corruption Vulnerability
- CVE-2021-26427 Microsoft Exchange Server Remote Code Execution Vulnerability
- CVE-2020-1971 OpenSSL: CVE-2020-1971 EDIPARTYNAME NULL pointer de-reference
- ADV990001 Latest Servicing Stack Updates
- ADV200011 Microsoft Guidance for Addressing Security Feature Bypass in GRUB

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
Windows 10 Professional SP1 64bit 1809	KB5006672	BeneVision CMS eGateway BeneVision CMS Viewer Hypervisor X CMS	windows10.0-kb5006672-x64_7044166433a0a9e2ffefe7608ad7d1fe05383c81.msu
Windows 10 Version 1607 for 32-bit Systems	KB5006669	BeneVision CMS Viewer BeneVision CMS Hypervisor X CMS	windows10.0-kb5006669-x86_891ad0792c8cd2745ca64fc03fd9a64d0dcc38ae.msu
Windows 10 Version 1607 for x64-based Systems	KB5006669	BeneVision CMS eGateway BeneVision CMS Viewer MLDAP Server Hypervisor X CMS	windows10.0-kb5006669-x64_aa5c931de237226eae4f333915750dbd998a8534.msu
Windows Server 2012 R2	KB5006729	BeneVision CMS eGateway	windows8.1-kb5006729-x86_4d05ea2c76d8a4d1179708932703ab095d9f16ef.msu
	KB5006714	BeneVision CMS Viewer BeneVision Mobile Server MLDAP Server	windows8.1-kb5006714-x64_403d2e21ee3f257f2127563ee5ea11a34093ec5d.msu
Windows Server 2016	KB5006669	BeneVision CMS eGateway MLDAP Server BeneVision Mobile	windows10.0-kb5006669-x64_aa5c931de237226eae4f333915750dbd998a8534.msu

		Server	
Windows 10 Version 1607 for x64-based Systems	KB5006669	iView	windows10.0-kb5006669-x64_aa5c931de237226eae4f333915750dbd998a8534.msu

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：2021-11-30