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

CVE Identifiers

- CVE-2021-36958 Windows Print Spooler Remote Code Execution Vulnerability
- CVE-2021-36950 Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability
- CVE-2021-36949 Microsoft Azure Active Directory Connect Authentication Bypass Vulnerability
- CVE-2021-36948 Windows Update Medic Service Elevation of Privilege Vulnerability
- CVE-2021-36947 Windows Print Spooler Remote Code Execution Vulnerability
- CVE-2021-36946 Microsoft Dynamics Business Central Cross-site Scripting Vulnerability
- CVE-2021-36945 Windows 10 Update Assistant Elevation of Privilege Vulnerability
- CVE-2021-36943 Azure CycleCloud Elevation of Privilege Vulnerability
- CVE-2021-36942 Windows LSA Spoofing Vulnerability
- CVE-2021-36941 Microsoft Word Remote Code Execution Vulnerability
- CVE-2021-36940 Microsoft SharePoint Server Spoofing Vulnerability
- CVE-2021-36938 Windows Cryptographic Primitives Library Information Disclosure Vulnerability
- CVE-2021-36937 Windows Media MPEG-4 Video Decoder Remote Code Execution Vulnerability
- CVE-2021-36936 Windows Print Spooler Remote Code Execution Vulnerability
- CVE-2021-36934 Windows Elevation of Privilege Vulnerability
- CVE-2021-36933 Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability
- CVE-2021-36932 Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability
- CVE-2021-36931 Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
- CVE-2021-36929 Microsoft Edge (Chromium-based) Information Disclosure Vulnerability
- CVE-2021-36928 Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
- CVE-2021-36927 Windows Digital TV Tuner device registration application Elevation of Privilege Vulnerability
- CVE-2021-36926 Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability
- CVE-2021-34537 Windows Bluetooth Driver Elevation of Privilege Vulnerability
- CVE-2021-34536 Storage Spaces Controller Elevation of Privilege Vulnerability
- CVE-2021-34535 Remote Desktop Client Remote Code Execution Vulnerability
- CVE-2021-34534 Windows MSHTML Platform Remote Code Execution Vulnerability

- CVE-2021-34533 Windows Graphics Component Font Parsing Remote Code Execution Vulnerability
- CVE-2021-34532 ASP.NET Core and Visual Studio Information Disclosure Vulnerability
- CVE-2021-34530 Windows Graphics Component Remote Code Execution Vulnerability
- CVE-2021-34527 Windows Print Spooler Remote Code Execution Vulnerability
- CVE-2021-34524 Microsoft Dynamics 365 (on-premises) Remote Code Execution Vulnerability
- CVE-2021-34487 Windows Event Tracing Elevation of Privilege Vulnerability
- CVE-2021-34486 Windows Event Tracing Elevation of Privilege Vulnerability
- CVE-2021-34485 .NET Core and Visual Studio Information Disclosure Vulnerability
- CVE-2021-34484 Windows User Profile Service Elevation of Privilege Vulnerability
- CVE-2021-34483 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2021-34481 Windows Print Spooler Remote Code Execution Vulnerability
- CVE-2021-34480 Scripting Engine Memory Corruption Vulnerability
- CVE-2021-34478 Microsoft Office Remote Code Execution Vulnerability
- CVE-2021-34476 Bowser.sys Denial of Service Vulnerability
- CVE-2021-34471 Microsoft Windows Defender Elevation of Privilege Vulnerability
- CVE-2021-34466 Windows Hello Security Feature Bypass Vulnerability
- CVE-2021-33781 Azure AD Security Feature Bypass Vulnerability
- CVE-2021-33762 Azure CycleCloud Elevation of Privilege Vulnerability
- CVE-2021-31984 Power BI Remote Code Execution Vulnerability
- CVE-2021-30604 Chromium: CVE-2021-30604 Use after free in ANGLE
- CVE-2021-30603 Chromium: CVE-2021-30603 Race in WebAudio
- CVE-2021-30602 Chromium: CVE-2021-30602 Use after free in WebRTC
- CVE-2021-30601 Chromium: CVE-2021-30601 Use after free in Extensions API
- CVE-2021-30599 Chromium: CVE-2021-30599 Type Confusion in V8
- CVE-2021-30598 Chromium: CVE-2021-30598 Type Confusion in V8
- CVE-2021-30597 Chromium: CVE-2021-30597 Use after free in Browser UI
- CVE-2021-30596 Chromium: CVE-2021-30596 Incorrect security UI in Navigation
- CVE-2021-30594 Chromium: CVE-2021-30594 Use after free in Page Info UI
- CVE-2021-30593 Chromium: CVE-2021-30593 Out of bounds read in Tab Strip
- CVE-2021-30592 Chromium: CVE-2021-30592 Out of bounds write in Tab Groups
- CVE-2021-30591 Chromium: CVE-2021-30591 Use after free in File System API
- CVE-2021-30590 Chromium: CVE-2021-30590 Heap buffer overflow in Bookmarks
- CVE-2021-30589 Chromium: CVE-2021-30589 Insufficient validation of untrusted input in Sharing
- CVE-2021-30588 Chromium: CVE-2021-30588 Type Confusion in V8
- CVE-2021-30587 Chromium: CVE-2021-30587 Inappropriate implementation in Compositing on Windows
- CVE-2021-30586 Chromium: CVE-2021-30586 Use after free in dialog box handling on Windows
- CVE-2021-30585 Chromium: CVE-2021-30585 Use after free in sensor handling
- CVE-2021-30584 Chromium: CVE-2021-30584 Incorrect security UI in Downloads
- CVE-2021-30583 Chromium: CVE-2021-30583 Insufficient policy enforcement in image handling on Windows
- CVE-2021-30582 Chromium: CVE-2021-30582 Inappropriate implementation in Animation
- CVE-2021-30581 Chromium: CVE-2021-30581 Use after free in DevTools

- CVE-2021-30580 Chromium: CVE-2021-30580 Insufficient policy enforcement in Android intents
- CVE-2021-30579 Chromium: CVE-2021-30579 Use after free in UI framework
- CVE-2021-30578 Chromium: CVE-2021-30578 Uninitialized Use in Media
- CVE-2021-30577 Chromium: CVE-2021-30577 Insufficient policy enforcement in Installer
- CVE-2021-30576 Chromium: CVE-2021-30576 Use after free in DevTools
- CVE-2021-30575 Chromium: CVE-2021-30575 Out of bounds read in Autofill
- CVE-2021-30574 Chromium: CVE-2021-30574 Use after free in protocol handling
- CVE-2021-30573 Chromium: CVE-2021-30573 Use after free in GPU
- CVE-2021-30572 Chromium: CVE-2021-30572 Use after free in Autofill
- CVE-2021-30571 Chromium: CVE-2021-30571 Insufficient policy enforcement in DevTools
- CVE-2021-30569 Chromium: CVE-2021-30569 Use after free in sqlite
- CVE-2021-30568 Chromium: CVE-2021-30568 Heap buffer overflow in WebGL
- CVE-2021-30567 Chromium: CVE-2021-30567 Use after free in DevTools
- CVE-2021-30566 Chromium: CVE-2021-30566 Stack buffer overflow in Printing
- CVE-2021-30565 Chromium: CVE-2021-30565 Out of bounds write in Tab Groups
- CVE-2021-30564 Chromium: CVE-2021-30564 Heap buffer overflow in WebXR
- CVE-2021-30563 Chromium: CVE-2021-30563 Type Confusion in V8
- CVE-2021-30562 Chromium: CVE-2021-30562 Use after free in WebSerial
- CVE-2021-30561 Chromium: CVE-2021-30561 Type Confusion in V8
- CVE-2021-30560 Chromium: CVE-2021-30560 Use after free in Blink XSLT
- CVE-2021-30559 Chromium: CVE-2021-30559 Out of bounds write in ANGLE
- CVE-2021-30541 Chromium: CVE-2021-30541 Use after free in V8
- CVE-2021-26433 Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability
- CVE-2021-26432 Windows Services for NFS ONCRPC XDR Driver Remote Code Execution Vulnerability
- CVE-2021-26431 Windows Recovery Environment Agent Elevation of Privilege Vulnerability
- CVE-2021-26430 Azure Sphere Denial of Service Vulnerability
- CVE-2021-26429 Azure Sphere Elevation of Privilege Vulnerability
- CVE-2021-26428 Azure Sphere Information Disclosure Vulnerability
- CVE-2021-26425 Windows Event Tracing Elevation of Privilege Vulnerability
- CVE-2021-26424 Windows TCP/IP Remote Code Execution Vulnerability
- CVE-2021-26423 .NET Core and Visual Studio Denial of Service Vulnerability
- CVE-2020-0765 Remote Desktop Connection Manager Information Disclosure Vulnerability
- ADV990001 Latest Servicing Stack Updates
- ADV210003 Mitigating NTLM Relay Attacks on Active Directory Certificate Services (AD CS)

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	KB5005030	BeneVision CMS eGateway BeneVision CMS Viewer, Hypervisor X CMS	windows10.0-kb5005030-x64_222160abfb75f543a693ca773dbcd0553ace6f03.msu
Windows 10 Version 1607 for 32-bit Systems	KB5005043	BeneVision CMS Viewer BeneVision CMS Hypervisor X CMS	windows10.0-kb5005043-x86_7e72b64b264e89ec87cf35af180b43c879b3ef5b.msu
Windows 10 Version 1607 for x64-based Systems	KB5005043	BeneVision CMS eGateway BeneVision CMS Viewer, MLDAP Server Hypervisor X CMS	windows10.0-kb5005043-x64_6e39252b88646ca55582da59e6f86a021d8b6ddd.msu
Windows Server 2012 R2	KB5005106	BeneVision CMS eGateway	windows8.1-kb5005106-x64_736921906ee56ea21d7e37e2b5446c78c53802d9.msu
	KB5005076	BeneVision CMS Viewer, BeneVision Mobile Server, MLDAP Server	windows8.1-kb5005076-x64_76a3e122bd0979784a084e4ccf0501c45661a83e.msu
Windows Server 2016	KB5005043	BeneVision CMS eGateway MLDAP Server BeneVision Mobile Server	windows10.0-kb5005043-x64_6e39252b88646ca55582da59e6f86a021d8b6ddd.msu
Windows 10 Version 1607 for x64-based Systems	KB5005043	iView	windows10.0-kb5005043-x64_6e39252b88646ca55582da59e6f86a021d8b6ddd.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：2021-9-21