

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, 2025. The following CVEs have been evaluated:

CVE Identifiers

- CVE-2025-62452 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
- CVE-2025-62219 Microsoft Wireless Provisioning System Elevation of Privilege Vulnerability
- CVE-2025-62218 Microsoft Wireless Provisioning System Elevation of Privilege Vulnerability
- CVE-2025-62217 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
- CVE-2025-62215 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2025-62213 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
- CVE-2025-62209 Windows License Manager Information Disclosure Vulnerability
- CVE-2025-62208 Windows License Manager Information Disclosure Vulnerability
- CVE-2025-60724 GDI+ Remote Code Execution Vulnerability
- CVE-2025-60723 DirectX Graphics Kernel Denial of Service Vulnerability
- CVE-2025-60721 Windows Administrator Protection Elevation of Privilege Vulnerability
- CVE-2025-60720 Windows Transport Driver Interface (TDI) Translation Driver Elevation of Privilege Vulnerability
- CVE-2025-60719 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
- CVE-2025-60718 Windows Administrator Protection Elevation of Privilege Vulnerability
- CVE-2025-60717 Windows Broadcast DVR User Service Elevation of Privilege Vulnerability
- CVE-2025-60716 DirectX Graphics Kernel Elevation of Privilege Vulnerability
- CVE-2025-60715 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
- CVE-2025-60714 Windows OLE Remote Code Execution Vulnerability
- CVE-2025-60713 Windows Routing and Remote Access Service (RRAS) Elevation of Privilege Vulnerability
- CVE-2025-60709 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2025-60708 Storvsp.sys Driver Denial of Service Vulnerability

- CVE-2025-60707 Multimedia Class Scheduler Service (MMCSS) Driver Elevation of Privilege Vulnerability
- CVE-2025-60706 Windows Hyper-V Information Disclosure Vulnerability
- CVE-2025-60705 Windows Client-Side Caching Elevation of Privilege Vulnerability
- CVE-2025-60704 Windows Kerberos Elevation of Privilege Vulnerability
- CVE-2025-60703 Windows Remote Desktop Services Elevation of Privilege Vulnerability
- CVE-2025-59515 Windows Broadcast DVR User Service Elevation of Privilege Vulnerability
- CVE-2025-59514 Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability
- CVE-2025-59513 Windows Bluetooth RFCOM Protocol Driver Information Disclosure Vulnerability
- CVE-2025-59512 Customer Experience Improvement Program (CEIP) Elevation of Privilege Vulnerability
- CVE-2025-59511 Windows WLAN Service Elevation of Privilege Vulnerability
- CVE-2025-59510 Windows Routing and Remote Access Service (RRAS) Denial of Service Vulnerability
- CVE-2025-59509 Windows Speech Recognition Information Disclosure Vulnerability
- CVE-2025-59508 Windows Speech Recognition Elevation of Privilege Vulnerability
- CVE-2025-59507 Windows Speech Runtime Elevation of Privilege Vulnerability
- CVE-2025-59506 DirectX Graphics Kernel Elevation of Privilege Vulnerability
- CVE-2025-59505 Windows Smart Card Reader Elevation of Privilege Vulnerability

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:

Product	OS	Hotfix	Download website	Necessary Pre-installed patch
BeneVision CMS	Windows 10 Professional SP1 64bit 1809	KB5068791	windows10.0-kb5068791-x64_a8b1b1b6c7b6b673c5a5f32772749eb2bb80c88b.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5068791	windows10.0-kb5068791-x64_a8b1b1b6c7b6b673c5a5f32772749eb2bb80c88b.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5070247 KB5068864	windows10.0-kb5070247-x86_9e6c55da58dc6c4cb97ef23bac2022afdc6c1fe5.msu windows10.0-kb5068864-x86_d021db4429873807f74146a55805d1aba6812b6e.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5070247 KB5068864	windows10.0-kb5070247-x64_3333d33e54ab21d7278f7cf6215bce448187dbc2.msu windows10.0-kb5068864-x64_8107e0baacab0ca8a7df12b299bc3dccb0765fa4.msu	KB4498947 KB4132216

	Windows Server 2016	KB5070247 KB5068864	windows10.0-kb5070247-x64_3333d33e54ab21d7278f7cf6215bce448187dbc2.msu windows10.0-kb5068864-x64_8107e0baacab0ca8a7df12b299bc3dccb0765fa4.msu	KB4498947 KB4132216
BeneVision CMS Viewer	Windows 10 Professional SP1 64bit 1809	KB5068791	windows10.0-kb5068791-x64_a8b1b1b6c7b6b673c5a5f32772749eb2bb80c88b.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5070247 KB5068864	windows10.0-kb5070247-x86_9e6c55da58dc6c4cb97ef23bac2022afdc6c1fe5.msu windows10.0-kb5068864-x86_d021db4429873807f74146a55805d1aba6812b6e.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5070247 KB5068864	windows10.0-kb5070247-x64_3333d33e54ab21d7278f7cf6215bce448187dbc2.msu windows10.0-kb5068864-x64_8107e0baacab0ca8a7df12b299bc3dccb0765fa4.msu	KB4498947 KB4132216
Hypervisor X CMS	Windows 10 Professional SP1 64bit 1809	KB5068791	windows10.0-kb5068791-x64_a8b1b1b6c7b6b673c5a5f32772749eb2bb80c88b.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5068791	windows10.0-kb5068791-x64_a8b1b1b6c7b6b673c5a5f32772749eb2bb80c88b.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5070247 KB5068864	windows10.0-kb5070247-x86_9e6c55da58dc6c4cb97ef23bac2022afdc6c1fe5.msu windows10.0-kb5068864-x86_d021db4429873807f74146a55805d1aba6812b6e.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5070247 KB5068864	windows10.0-kb5070247-x64_3333d33e54ab21d7278f7cf6215bce448187dbc2.msu windows10.0-kb5068864-x64_8107e0baacab0ca8a7df12b299bc3dccb0765fa4.msu	KB4498947 KB4132216
eGateway	Windows 10 Professional SP1 64bit 1809	KB5068791	windows10.0-kb5068791-x64_a8b1b1b6c7b6b673c5a5f32772749eb2bb80c88b.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5068791	windows10.0-kb5068791-x64_a8b1b1b6c7b6b673c5a5f32772749eb2bb80c88b.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for x64-based	KB5070247 KB5068864	windows10.0-kb5070247-x64_3333d33e54ab21d7278f7cf6215bce448187dbc2.msu windows10.0-kb5068864-x64_8107e0baacab0ca8a7df12b299bc3dccb0765fa4.msu	KB4498947 KB4132216
	Windows Server 2016	KB5070247 KB5068864	windows10.0-kb5070247-x64_3333d33e54ab21d7278f7cf6215bce448187dbc2.msu windows10.0-kb5068864-x64_8107e0baacab0ca8a7df12b299bc3dccb0765fa4.msu	KB4498947 KB4132216
MLDAP Server	Windows 10 1607 for x64-based	KB5070247 KB5068864	windows10.0-kb5070247-x64_3333d33e54ab21d7278f7cf6215bce448187dbc2.msu windows10.0-kb5068864-x64_8107e0baacab0ca8a7df12b299bc3dccb0765fa4.msu	KB4498947 KB4132216

	Windows Server 2016	KB5070247 KB5068864	windows10.0-kb5070247-x64_3333d33e54ab21d7278f7cf6215bce448187dbc2.msu windows10.0-kb5068864-x64_8107e0baacab0ca8a7df12b299bc3dccb0765fa4.msu	KB4498947 KB4132216
	Windows Server 2019	KB5068791	windows10.0-kb5068791-x64_a8b1b1b6c7b6b673c5a5f32772749eb2bb80c88b.msu	KB5005112 KB5003243 KB4587735
BeneVision Mobile Server	Windows Server 2016	KB5070247 KB5068864	windows10.0-kb5070247-x64_3333d33e54ab21d7278f7cf6215bce448187dbc2.msu windows10.0-kb5068864-x64_8107e0baacab0ca8a7df12b299bc3dccb0765fa4.msu	KB4498947 KB4132216
	Windows Server 2019	KB5068791	windows10.0-kb5068791-x64_a8b1b1b6c7b6b673c5a5f32772749eb2bb80c88b.msu	KB5005112 KB5003243 KB4587735
iView	Windows 10 1607 for x64-based	KB5070247 KB5068864	windows10.0-kb5070247-x64_3333d33e54ab21d7278f7cf6215bce448187dbc2.msu windows10.0-kb5068864-x64_8107e0baacab0ca8a7df12b299bc3dccb0765fa4.msu	KB4498947 KB4132216

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: 2025-12-2