Security Patches for Mindray Products Running on Windows OS (May, 2025)

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 May, 2025. The following CVEs have been evaluated:

CVE Identifiers

- CVE-2025-32709 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
- CVE-2025-32707 NTFS Elevation of Privilege Vulnerability
- CVE-2025-32701 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2025-30400 Microsoft DWM Core Library Elevation of Privilege Vulnerability
- CVE-2025-30397 Scripting Engine Memory Corruption Vulnerability
- CVE-2025-30394 Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability
- CVE-2025-30388 Windows Graphics Component Remote Code Execution Vulnerability
- CVE-2025-30385 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2025-29974 Windows Kernel Information Disclosure Vulnerability
- CVE-2025-29971 Web Threat Defense (WTD.sys) Denial of Service Vulnerability
- CVE-2025-29970 Microsoft Brokering File System Elevation of Privilege Vulnerability
- CVE-2025-29969 MS-EVEN RPC Remote Code Execution Vulnerability
- CVE-2025-29968 Active Directory Certificate Services (AD CS) Denial of Service Vulnerability
- CVE-2025-29967 Remote Desktop Client Remote Code Execution Vulnerability
- CVE-2025-29966 Remote Desktop Client Remote Code Execution Vulnerability
- CVE-2025-29964 Windows Media Remote Code Execution Vulnerability
- CVE-2025-29963 Windows Media Remote Code Execution Vulnerability
- CVE-2025-29962 Windows Media Remote Code Execution Vulnerability
- CVE-2025-29961 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-29960 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-29959 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-29958 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-29957 Windows Deployment Services Denial of Service Vulnerability
- CVE-2025-29956 Windows SMB Information Disclosure Vulnerability

- CVE-2025-29955 Windows Hyper-V Denial of Service Vulnerability
- CVE-2025-29954 Windows Lightweight Directory Access Protocol (LDAP) Denial of Service Vulnerability
- CVE-2025-29842 UrlMon Security Feature Bypass Vulnerability
- CVE-2025-29841 Universal Print Management Service Elevation of Privilege Vulnerability
- CVE-2025-29840 Windows Media Remote Code Execution Vulnerability
- CVE-2025-29839 Windows Multiple UNC Provider Driver Information Disclosure Vulnerability
- CVE-2025-29838 Windows ExecutionContext Driver Elevation of Privilege Vulnerability
- CVE-2025-29837 Windows Installer Information Disclosure Vulnerability
- CVE-2025-29836 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-29835 Windows Remote Access Connection Manager Information Disclosure Vulnerability
- CVE-2025-29833 Microsoft Virtual Machine Bus (VMBus) Remote Code Execution Vulnerability
- CVE-2025-29832 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-29831 Windows Remote Desktop Services Remote Code Execution Vulnerability
- CVE-2025-29830 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-29829 Windows Trusted Runtime Interface Driver Information Disclosure Vulnerability
- CVE-2025-27468 Windows Kernel-Mode Driver Elevation of Privilege Vulnerability
- CVE-2025-26677 Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability
- CVE-2025-24063 Kernel Streaming Service Driver 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	KB5058392	windows10.0-kb5058392-x64_2881b28817b6e714e61b61a50de9f68605f02bd2.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5058392	windows10.0-kb5058392-x64_2881b28817b6e714e61b61a50de9f68605f02bd2.msu	KB5005112 KB5003243 KB4587735

	Windows 10 1607 for 32-bit	KB5058383	windows10.0-kb5058383-x86_9ae7fb9ef009e05b8c3cb410881be1bfaa053bf0.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5058383	windows10.0-kb5058383-x64_f2e34deb03d8284d2bc746589ec83fd20747edd0.msu	KB4498947 KB4132216
	Windows Server 2016	KB5058383	windows10.0-kb5058383-x64_f2e34deb03d8284d2bc746589ec83fd20747edd0.msu	KB4498947 KB4132216
BeneVision CMS Viewer	Windows 10 Professional SP1 64bit 1809	KB5058392	windows10.0-kb5058392-x64_2881b28817b6e714e61b61a50de9f68605f02bd2.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5058383	windows10.0-kb5058383-x86_9ae7fb9ef009e05b8c3cb410881be1bfaa053bf0.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5058383	windows10.0-kb5058383-x64_f2e34deb03d8284d2bc746589ec83fd20747edd0.msu	KB4498947 KB4132216
Hypervisor X CMS	Windows 10 Professional SP1 64bit 1809	KB5058392	windows10.0-kb5058392-x64_2881b28817b6e714e61b61a50de9f68605f02bd2.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5058392	windows10.0-kb5058392-x64_2881b28817b6e714e61b61a50de9f68605f02bd2.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5058383	windows10.0-kb5058383-x86_9ae7fb9ef009e05b8c3cb410881be1bfaa053bf0.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5058383	windows10.0-kb5058383-x64_f2e34deb03d8284d2bc746589ec83fd20747edd0.msu	KB4498947 KB4132216
eGateway	Windows 10 Professional SP1 64bit 1809	KB5058392	windows10.0-kb5058392-x64_2881b28817b6e714e61b61a50de9f68605f02bd2.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5058392	windows10.0-kb5058392-x64_2881b28817b6e714e61b61a50de9f68605f02bd2.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for x64-based	KB5058383	windows10.0-kb5058383-x64_f2e34deb03d8284d2bc746589ec83fd20747edd0.msu	KB4498947 KB4132216
	Windows Server 2016	KB5058383	windows10.0-kb5058383-x64_f2e34deb03d8284d2bc746589ec83fd20747edd0.msu	KB4498947 KB4132216
MLDAP Server	Windows 10 1607 for x64-based	KB5058383	windows10.0-kb5058383-x64_f2e34deb03d8284d2bc746589ec83fd20747edd0.msu	KB4498947 KB4132216
	Windows Server 2016	KB5058383	windows10.0-kb5058383-x64_f2e34deb03d8284d2bc746589ec83fd20747edd0.msu	KB4498947 KB4132216
	Windows Server 2019	KB5058392	windows10.0-kb5058392-x64_2881b28817b6e714e61b61a50de9f68605f02bd2.msu	KB5005112 KB5003243 KB4587735
BeneVision Mobile Server	Windows Server 2016	KB5058383	windows10.0-kb5058383-x64_f2e34deb03d8284d2bc746589ec83fd20747edd0.msu	KB4498947 KB4132216

	Windows Server 2019	KB5058392	windows10.0-kb5058392-x64_2881b28817b6e714e61b61a50de9f68605f02bd2.msu	KB5005112 KB5003243 KB4587735
iView	Windows 10 1607 for x64-based	KB5058383	windows10.0-kb5058383-x64_f2e34deb03d8284d2bc746589ec83fd20747edd0.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：2025-6-11