Security Patches for Mindray Products Running on Windows OS (July, 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 July, 2025. The following CVEs have been evaluated:

CVE Identifiers

- CVE-2025-49760 Windows Storage Spoofing Vulnerability
- CVE-2025-49753 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
- CVE-2025-49744 Windows Graphics Component Elevation of Privilege Vulnerability
- CVE-2025-49742 Windows Graphics Component Remote Code Execution Vulnerability
- CVE-2025-49740 Windows SmartScreen Security Feature Bypass Vulnerability
- CVE-2025-49735 Windows KDC Proxy Service (KPSSVC) Remote Code Execution Vulnerability
- CVE-2025-49733 Win32k Elevation of Privilege Vulnerability
- CVE-2025-49732 Windows Graphics Component Elevation of Privilege Vulnerability
- CVE-2025-49730 Microsoft Windows QoS Scheduler Driver Elevation of Privilege Vulnerability
- CVE-2025-49729 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
- CVE-2025-49727 Win32k Elevation of Privilege Vulnerability
- CVE-2025-49726 Windows Notification Elevation of Privilege Vulnerability
- CVE-2025-49725 Windows Notification Elevation of Privilege Vulnerability
- CVE-2025-49724 Windows Connected Devices Platform Service Remote Code Execution Vulnerability
- CVE-2025-49723 Windows StateRepository API Server file Tampering Vulnerability
- CVE-2025-49722 Windows Print Spooler Denial of Service Vulnerability
- CVE-2025-49721 Windows Fast FAT File System Driver Elevation of Privilege Vulnerability
- CVE-2025-49716 Windows Netlogon Denial of Service Vulnerability
- CVE-2025-49694 Microsoft Brokering File System Elevation of Privilege Vulnerability
- CVE-2025-49693 Microsoft Brokering File System Elevation of Privilege Vulnerability
- CVE-2025-49691 Windows Miracast Wireless Display Remote Code Execution Vulnerability
- CVE-2025-49690 Capability Access Management Service (camsvc) Elevation of Privilege Vulnerability
- CVE-2025-49689 Microsoft Virtual Hard Disk Elevation of Privilege Vulnerability
- CVE-2025-49688 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability

- CVE-2025-49687 Windows Input Method Editor (IME) Elevation of Privilege Vulnerability
- CVE-2025-49686 Windows TCP/IP Driver Elevation of Privilege Vulnerability
- CVE-2025-49685 Windows Search Service Elevation of Privilege Vulnerability
- CVE-2025-49684 Windows Storage Port Driver Information Disclosure Vulnerability
- CVE-2025-49683 Microsoft Virtual Hard Disk Remote Code Execution Vulnerability
- CVE-2025-49682 Windows Media Elevation of Privilege Vulnerability
- CVE-2025-49681 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-49680 Windows Performance Recorder (WPR) Denial of Service Vulnerability
- CVE-2025-49679 Windows Shell Elevation of Privilege Vulnerability
- CVE-2025-49678 NTFS Elevation of Privilege Vulnerability
- CVE-2025-49676 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
- CVE-2025-49675 Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability
- CVE-2025-49674 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
- CVE-2025-49673 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
- CVE-2025-49672 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
- CVE-2025-49671 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-49670 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
- CVE-2025-49669 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
- CVE-2025-49668 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
- CVE-2025-49667 Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability
- CVE-2025-49666 Windows Server Setup and Boot Event Collection Remote Code Execution Vulnerability
- CVE-2025-49665 Workspace Broker Elevation of Privilege Vulnerability
- CVE-2025-49664 Windows User-Mode Driver Framework Host Information Disclosure Vulnerability
- CVE-2025-49663 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
- CVE-2025-49661 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
- CVE-2025-49660 Windows Event Tracing Elevation of Privilege Vulnerability
- CVE-2025-49659 Windows Transport Driver Interface (TDI) Translation Driver Elevation of Privilege Vulnerability
- CVE-2025-49658 Windows Transport Driver Interface (TDI) Translation Driver Information Disclosure Vulnerability
- CVE-2025-49657 Windows Routing and Remote Access Service (RRAS) Remote

Code Execution Vulnerability
- CVE-2025-48824 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
- CVE-2025-48823 Windows Cryptographic Services Information Disclosure Vulnerability
- CVE-2025-48822 Windows Hyper-V Discrete Device Assignment (DDA) Remote Code Execution Vulnerability
- CVE-2025-48821 Windows Universal Plug and Play (UPnP) Device Host Elevation of Privilege Vulnerability
- CVE-2025-48820 Windows AppX Deployment Service Elevation of Privilege Vulnerability
- CVE-2025-48819 Windows Universal Plug and Play (UPnP) Device Host Elevation of Privilege Vulnerability
- CVE-2025-48818 BitLocker Security Feature Bypass Vulnerability
- CVE-2025-48817 Remote Desktop Client Remote Code Execution Vulnerability
- CVE-2025-48816 HID Class Driver Elevation of Privilege Vulnerability
- CVE-2025-48815 Windows Simple Search and Discovery Protocol (SSDP) Service Elevation of Privilege Vulnerability
- CVE-2025-48814 Remote Desktop Licensing Service Security Feature Bypass Vulnerability
- CVE-2025-48811 Windows Virtualization-Based Security (VBS) Enclave Elevation of Privilege Vulnerability
- CVE-2025-48809 Windows Secure Kernel Mode Information Disclosure Vulnerability
- CVE-2025-48808 Windows Kernel Information Disclosure Vulnerability
- CVE-2025-48806 Microsoft MPEG-2 Video Extension Remote Code Execution Vulnerability
- CVE-2025-48805 Microsoft MPEG-2 Video Extension Remote Code Execution Vulnerability
- CVE-2025-48804 BitLocker Security Feature Bypass Vulnerability
- CVE-2025-48803 Windows Virtualization-Based Security (VBS) Elevation of Privilege Vulnerability
- CVE-2025-48800 BitLocker Security Feature Bypass Vulnerability
- CVE-2025-48799 Windows Update Service Elevation of Privilege Vulnerability
- CVE-2025-48003 BitLocker Security Feature Bypass Vulnerability
- CVE-2025-48002 Windows Hyper-V Information Disclosure Vulnerability
- CVE-2025-48001 BitLocker Security Feature Bypass Vulnerability
- CVE-2025-48000 Windows Connected Devices Platform Service Elevation of Privilege Vulnerability
- CVE-2025-47999 Windows Hyper-V Denial of Service Vulnerability
- CVE-2025-47998 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
- CVE-2025-47996 Windows MBT Transport Driver Elevation of Privilege Vulnerability
- CVE-2025-47993 Microsoft PC Manager Elevation of Privilege Vulnerability
- CVE-2025-47991 Windows Input Method Editor (IME) Elevation of Privilege Vulnerability
- CVE-2025-47987 Credential Security Support Provider Protocol (CredSSP) Elevation of Privilege Vulnerability
- CVE-2025-47986 Universal Print Management Service Elevation of Privilege

Vulnerability

- CVE-2025-47985 Windows Event Tracing Elevation of Privilege Vulnerability
- CVE-2025-47984 Windows GDI Information Disclosure Vulnerability
- CVE-2025-47982 Windows Storage VSP Driver Elevation of Privilege Vulnerability
- CVE-2025-47981 SPNEGO Extended Negotiation (NEGOEX) Security Mechanism Remote Code Execution Vulnerability
- CVE-2025-47980 Windows Imaging Component Information Disclosure Vulnerability
- CVE-2025-47978 Windows Kerberos Denial of Service Vulnerability
- CVE-2025-47976 Windows Simple Search and Discovery Protocol (SSDP) Service Elevation of Privilege Vulnerability
- CVE-2025-47975 Windows Simple Search and Discovery Protocol (SSDP) Service Elevation of Privilege Vulnerability
- CVE-2025-47973 Microsoft Virtual Hard Disk Elevation of Privilege Vulnerability
- CVE-2025-47972 Windows Input Method Editor (IME) Elevation of Privilege Vulnerability
- CVE-2025-47971 Microsoft Virtual Hard Disk Elevation of Privilege Vulnerability
- CVE-2025-36357 AMD: CVE-2025-36357 Transient Scheduler Attack in L1 Data Queue
- CVE-2025-33054 Remote Desktop Spoofing Vulnerability

CVE-2024-36350 AMD: CVE-2024-36350 Transient Scheduler Attack in Store Queue

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	KB5062557	windows10.0-kb5062557-x64_cf62475a0842bb1dc1f73180bc478ad7d8d9c7ab.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5062557	windows10.0-kb5062557-x64_cf62475a0842bb1dc1f73180bc478ad7d8d9c7ab.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5062560	windows10.0-kb5062560-x86_15157b9fdf2cb3fbe2cbea6f54f7d5a7e09ef886.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5062560	windows10.0-kb5062560-x64_eab2ba1274fcf4fc3169e7dcfff8be1aeca1de08.msu	KB4498947 KB4132216
	Windows Server 2016	KB5062560	windows10.0-kb5062560-x64_eab2ba1274fcf4fc3169e7dcfff8be1aeca1de08.msu	KB4498947 KB4132216
BeneVision CMS Viewer	Windows 10 Professional SP1 64bit 1809	KB5062557	windows10.0-kb5062557-x64_cf62475a0842bb1dc1f73180bc478ad7d8d9c7ab.msu	KB5005112 KB5003243 KB4587735

	Windows 10 1607 for 32-bit	KB5062560	windows10.0-kb5062560-x86_15157b9fdf2cb3fbe2cbea6f54f7d5a7e09ef886.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5062560	windows10.0-kb5062560-x64_eab2ba1274fcf4fc3169e7dcfff8be1aeca1de08.msu	KB4498947 KB4132216
Hypervisor X CMS	Windows 10 Professional SP1 64bit 1809	KB5062557	windows10.0-kb5062557-x64_cf62475a0842bb1dc1f73180bc478ad7d8d9c7ab.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5062557	windows10.0-kb5062557-x64_cf62475a0842bb1dc1f73180bc478ad7d8d9c7ab.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5062560	windows10.0-kb5062560-x86_15157b9fdf2cb3fbe2cbea6f54f7d5a7e09ef886.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5062560	windows10.0-kb5062560-x64_eab2ba1274fcf4fc3169e7dcfff8be1aeca1de08.msu	KB4498947 KB4132216
eGateway	Windows 10 Professional SP1 64bit 1809	KB5062557	windows10.0-kb5062557-x64_cf62475a0842bb1dc1f73180bc478ad7d8d9c7ab.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5062557	windows10.0-kb5062557-x64_cf62475a0842bb1dc1f73180bc478ad7d8d9c7ab.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for x64-based	KB5062560	windows10.0-kb5062560-x64_eab2ba1274fcf4fc3169e7dcfff8be1aeca1de08.msu	KB4498947 KB4132216
	Windows Server 2016	KB5062560	windows10.0-kb5062560-x64_eab2ba1274fcf4fc3169e7dcfff8be1aeca1de08.msu	KB4498947 KB4132216
MLDAP Server	Windows 10 1607 for x64-based	KB5062560	windows10.0-kb5062560-x64_eab2ba1274fcf4fc3169e7dcfff8be1aeca1de08.msu	KB4498947 KB4132216
	Windows Server 2016	KB5062560	windows10.0-kb5062560-x64_eab2ba1274fcf4fc3169e7dcfff8be1aeca1de08.msu	KB4498947 KB4132216
	Windows Server 2019	KB5062557	windows10.0-kb5062557-x64_cf62475a0842bb1dc1f73180bc478ad7d8d9c7ab.msu	KB5005112 KB5003243 KB4587735
BeneVision Mobile Server	Windows Server 2016	KB5062560	windows10.0-kb5062560-x64_eab2ba1274fcf4fc3169e7dcfff8be1aeca1de08.msu	KB4498947 KB4132216
	Windows Server 2019	KB5062557	windows10.0-kb5062557-x64_cf62475a0842bb1dc1f73180bc478ad7d8d9c7ab.msu	KB5005112 KB5003243 KB4587735
iView	Windows 10 1607 for x64-based	KB5062560	windows10.0-kb5062560-x64_eab2ba1274fcf4fc3169e7dcfff8be1aeca1de08.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：2025-7-29