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

CVE Identifiers

- CVE-2025-29824 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2025-29812 DirectX Graphics Kernel Elevation of Privilege Vulnerability
- CVE-2025-29811 Windows Mobile Broadband Driver Elevation of Privilege Vulnerability
- CVE-2025-29810 Active Directory Domain Services Elevation of Privilege Vulnerability
- CVE-2025-29809 Windows Kerberos Security Feature Bypass Vulnerability
- CVE-2025-29808 Windows Cryptographic Services Information Disclosure Vulnerability
- CVE-2025-27743 Microsoft System Center Elevation of Privilege Vulnerability
- CVE-2025-27742 NTFS Information Disclosure Vulnerability
- CVE-2025-27741 NTFS Elevation of Privilege Vulnerability
- CVE-2025-27740 Active Directory Certificate Services Elevation of Privilege Vulnerability
- CVE-2025-27739 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2025-27738 Windows Resilient File System (ReFS) Information Disclosure Vulnerability
- CVE-2025-27737 Windows Security Zone Mapping Security Feature Bypass Vulnerability
- CVE-2025-27736 Windows Power Dependency Coordinator Information Disclosure Vulnerability
- CVE-2025-27735 Windows Virtualization-Based Security (VBS) Security Feature Bypass Vulnerability
- CVE-2025-27733 NTFS Elevation of Privilege Vulnerability
- CVE-2025-27732 Windows Graphics Component Elevation of Privilege Vulnerability
- CVE-2025-27731 Microsoft OpenSSH for Windows Elevation of Privilege Vulnerability
- CVE-2025-27730 Windows Digital Media Elevation of Privilege Vulnerability
- CVE-2025-27729 Windows Shell Remote Code Execution Vulnerability
- CVE-2025-27728 Windows Kernel-Mode Driver Elevation of Privilege Vulnerability
- CVE-2025-27727 Windows Installer Elevation of Privilege Vulnerability
- CVE-2025-27492 Windows Secure Channel Elevation of Privilege Vulnerability
- CVE-2025-27491 Windows Hyper-V Remote Code Execution Vulnerability
- CVE-2025-27490 Windows Bluetooth Service Elevation of Privilege Vulnerability

- CVE-2025-27487 Remote Desktop Client Remote Code Execution Vulnerability
- CVE-2025-27486 Windows Standards-Based Storage Management Service Denial of Service Vulnerability
- CVE-2025-27485 Windows Standards-Based Storage Management Service Denial of Service Vulnerability
- CVE-2025-27484 Windows Universal Plug and Play (UPnP) Device Host Elevation of Privilege Vulnerability
- CVE-2025-27483 NTFS Elevation of Privilege Vulnerability
- CVE-2025-27482 Windows Remote Desktop Services Remote Code Execution Vulnerability
- CVE-2025-27481 Windows Telephony Service Remote Code Execution Vulnerability
- CVE-2025-27480 Windows Remote Desktop Services Remote Code Execution Vulnerability
- CVE-2025-27479 Kerberos Key Distribution Proxy Service Denial of Service Vulnerability
- CVE-2025-27478 Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability
- CVE-2025-27476 Windows Digital Media Elevation of Privilege Vulnerability
- CVE-2025-27475 Windows Update Stack Elevation of Privilege Vulnerability
- CVE-2025-27474 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-27473 HTTP.sys Denial of Service Vulnerability
- CVE-2025-27471 Microsoft Streaming Service Denial of Service Vulnerability
- CVE-2025-27470 Windows Standards-Based Storage Management Service Denial of Service Vulnerability
- CVE-2025-27469 Windows Lightweight Directory Access Protocol (LDAP) Denial of Service Vulnerability
- CVE-2025-27467 Windows Digital Media Elevation of Privilege Vulnerability
- CVE-2025-26688 Microsoft Virtual Hard Disk Elevation of Privilege Vulnerability
- CVE-2025-26687 Win32k Elevation of Privilege Vulnerability
- CVE-2025-26686 Windows TCP/IP Remote Code Execution Vulnerability
- CVE-2025-26682 ASP.NET Core and Visual Studio Denial of Service Vulnerability
- CVE-2025-26681 Win32k Elevation of Privilege Vulnerability
- CVE-2025-26680 Windows Standards-Based Storage Management Service Denial of Service Vulnerability
- CVE-2025-26679 RPC Endpoint Mapper Service Elevation of Privilege Vulnerability
- CVE-2025-26678 Windows Defender Application Control Security Feature Bypass Vulnerability
- CVE-2025-26676 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-26675 Windows Subsystem for Linux Elevation of Privilege Vulnerability
- CVE-2025-26674 Windows Media Remote Code Execution Vulnerability
- CVE-2025-26673 Windows Lightweight Directory Access Protocol (LDAP) Denial of Service Vulnerability
- CVE-2025-26672 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-26671 Windows Remote Desktop Services Remote Code Execution Vulnerability

- CVE-2025-26670 Lightweight Directory Access Protocol (LDAP) Client Remote Code Execution Vulnerability
- CVE-2025-26669 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-26668 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
- CVE-2025-26667 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-26666 Windows Media Remote Code Execution Vulnerability
- CVE-2025-26665 Windows upnphost.dll Elevation of Privilege Vulnerability
- CVE-2025-26664 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-26663 Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
- CVE-2025-26652 Windows Standards-Based Storage Management Service Denial of Service Vulnerability
- CVE-2025-26651 Windows Local Session Manager (LSM) Denial of Service Vulnerability
- CVE-2025-26649 Windows Secure Channel Elevation of Privilege Vulnerability
- CVE-2025-26648 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2025-26647 Windows Kerberos Elevation of Privilege Vulnerability
- CVE-2025-26644 Windows Hello Spoofing Vulnerability
- CVE-2025-26641 Microsoft Message Queuing (MSMQ) Denial of Service Vulnerability
- CVE-2025-26640 Windows Digital Media Elevation of Privilege Vulnerability
- CVE-2025-26639 Windows USB Print Driver Elevation of Privilege Vulnerability
- CVE-2025-26637 BitLocker Security Feature Bypass Vulnerability
- CVE-2025-26635 Windows Hello Security Feature Bypass Vulnerability
- CVE-2025-24074 Microsoft DWM Core Library Elevation of Privilege Vulnerability
- CVE-2025-24073 Microsoft DWM Core Library Elevation of Privilege Vulnerability
- CVE-2025-24062 Microsoft DWM Core Library Elevation of Privilege Vulnerability
- CVE-2025-24060 Microsoft DWM Core Library Elevation of Privilege Vulnerability
- CVE-2025-24058 Windows DWM Core Library Elevation of Privilege Vulnerability
- CVE-2025-21222 Windows Telephony Service Remote Code Execution Vulnerability
- CVE-2025-21221 Windows Telephony Service Remote Code Execution Vulnerability
- CVE-2025-21205 Windows Telephony Service Remote Code Execution Vulnerability
- CVE-2025-21204 Windows Process Activation Elevation of Privilege Vulnerability
- CVE-2025-21203 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-21197 Windows NTFS Information Disclosure Vulnerability
- CVE-2025-21191 Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability
- CVE-2025-21174 Windows Standards-Based Storage Management Service Denial of Service 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	KB5055519	windows10.0-kb5055519-x64_075404b22fd325768631d15699de8f6e6af5a352.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5055519	windows10.0-kb5055519-x64_075404b22fd325768631d15699de8f6e6af5a352.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5055521	windows10.0-kb5055521-x86_2fac5c0800b2269f75b3f48c02c282ef57492777.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5055521	windows10.0-kb5055521-x64_41090eb90fce0c94b6a9e1a986b0c4810befeea1.msu	KB4498947 KB4132216
	Windows Server 2016	KB5055521	windows10.0-kb5055521-x64_41090eb90fce0c94b6a9e1a986b0c4810befeea1.msu	KB4498947 KB4132216
BeneVision CMS Viewer	Windows 10 Professional SP1 64bit 1809	KB5055519	windows10.0-kb5055519-x64_075404b22fd325768631d15699de8f6e6af5a352.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5055521	windows10.0-kb5055521-x86_2fac5c0800b2269f75b3f48c02c282ef57492777.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5055521	windows10.0-kb5055521-x64_41090eb90fce0c94b6a9e1a986b0c4810befeea1.msu	KB4498947 KB4132216
Hypervisor X CMS	Windows 10 Professional SP1 64bit 1809	KB5055519	windows10.0-kb5055519-x64_075404b22fd325768631d15699de8f6e6af5a352.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5055519	windows10.0-kb5055519-x64_075404b22fd325768631d15699de8f6e6af5a352.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5055521	windows10.0-kb5055521-x86_2fac5c0800b2269f75b3f48c02c282ef57492777.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5055521	windows10.0-kb5055521-x64_41090eb90fce0c94b6a9e1a986b0c4810befeea1.msu	KB4498947 KB4132216
eGateway	Windows 10 Professional SP1 64bit 1809	KB5055519	windows10.0-kb5055519-x64_075404b22fd325768631d15699de8f6e6af5a352.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5055519	windows10.0-kb5055519-x64_075404b22fd325768631d15699de8f6e6af5a352.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for x64-	KB5055521	windows10.0-kb5055521-x64_41090eb90fce0c94b6a9e1a986b0c4810befeea1.msu	KB4498947 KB4132216

	based			
	Windows Server 2016	KB5055521	windows10.0-kb5055521-x64_41090eb90fce0c94b6a9e1a986b0c4810befeea1.msu	KB4498947 KB4132216
MLDAP Server	Windows 10 1607 for x64-based	KB5055521	windows10.0-kb5055521-x64_41090eb90fce0c94b6a9e1a986b0c4810befeea1.msu	KB4498947 KB4132216
	Windows Server 2016	KB5055521	windows10.0-kb5055521-x64_41090eb90fce0c94b6a9e1a986b0c4810befeea1.msu	KB4498947 KB4132216
	Windows Server 2019	KB5055519	windows10.0-kb5055519-x64_075404b22fd325768631d15699de8f6e6af5a352.msu	KB5005112 KB5003243 KB4587735
BeneVision Mobile Server	Windows Server 2016	KB5055521	windows10.0-kb5055521-x64_41090eb90fce0c94b6a9e1a986b0c4810befeea1.msu	KB4498947 KB4132216
	Windows Server 2019	KB5055519	windows10.0-kb5055519-x64_075404b22fd325768631d15699de8f6e6af5a352.msu	KB5005112 KB5003243 KB4587735
iView	Windows 10 1607 for x64-based	KB5055521	windows10.0-kb5055521-x64_41090eb90fce0c94b6a9e1a986b0c4810befeea1.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：2025-5-8