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

CVE Identifiers

- CVE-2025-59220 Windows Bluetooth Service Elevation of Privilege Vulnerability
- CVE-2025-59216 Windows Graphics Component Elevation of Privilege Vulnerability
- CVE-2025-59215 Windows Graphics Component Elevation of Privilege Vulnerability
- CVE-2025-55236 Graphics Kernel Remote Code Execution Vulnerability
- CVE-2025-55234 Windows SMB Elevation of Privilege Vulnerability
- CVE-2025-55228 Windows Graphics Component Remote Code Execution Vulnerability
- CVE-2025-55226 Graphics Kernel Remote Code Execution Vulnerability
- CVE-2025-55225 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-55224 Windows Hyper-V Remote Code Execution Vulnerability
- CVE-2025-55223 DirectX Graphics Kernel Elevation of Privilege Vulnerability
- CVE-2025-54919 Windows Graphics Component Remote Code Execution Vulnerability
- CVE-2025-54918 Windows NTLM Elevation of Privilege Vulnerability
- CVE-2025-54917 MapUrlToZone Security Feature Bypass Vulnerability
- CVE-2025-54916 Windows NTFS Remote Code Execution Vulnerability
- CVE-2025-54915 Windows Defender Firewall Service Elevation of Privilege Vulnerability
- CVE-2025-54913 Windows UI XAML Maps MapControlSettings Elevation of Privilege Vulnerability
- CVE-2025-54912 Windows BitLocker Elevation of Privilege Vulnerability
- CVE-2025-54911 Windows BitLocker Elevation of Privilege Vulnerability
- CVE-2025-54895 SPNEGO Extended Negotiation (NEGOEX) Security Mechanism Elevation of Privilege Vulnerability
- CVE-2025-54894 Local Security Authority Subsystem Service Elevation of Privilege Vulnerability
- CVE-2025-54116 Windows MultiPoint Services Elevation of Privilege Vulnerability
- CVE-2025-54115 Windows Hyper-V Elevation of Privilege Vulnerability
- CVE-2025-54114 Windows Connected Devices Platform Service (Cdpsvc) Denial of Service Vulnerability
- CVE-2025-54113 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
- CVE-2025-54112 Microsoft Virtual Hard Disk Elevation of Privilege Vulnerability

- CVE-2025-54111 Windows UI XAML Phone DatePickerFlyout Elevation of Privilege Vulnerability
- CVE-2025-54110 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2025-54109 Windows Defender Firewall Service Elevation of Privilege Vulnerability
- CVE-2025-54108 Capability Access Management Service (camsvc) Elevation of Privilege Vulnerability
- CVE-2025-54107 MapUrlToZone Security Feature Bypass Vulnerability
- CVE-2025-54106 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
- CVE-2025-54105 Microsoft Brokering File System Elevation of Privilege Vulnerability
- CVE-2025-54104 Windows Defender Firewall Service Elevation of Privilege Vulnerability
- CVE-2025-54103 Windows Management Service Elevation of Privilege Vulnerability
- CVE-2025-54102 Windows Connected Devices Platform Service Elevation of Privilege Vulnerability
- CVE-2025-54101 Windows SMB Client Remote Code Execution Vulnerability
- CVE-2025-54099 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
- CVE-2025-54098 Windows Hyper-V Elevation of Privilege Vulnerability
- CVE-2025-54097 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-54096 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-54095 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-54094 Windows Defender Firewall Service Elevation of Privilege Vulnerability
- CVE-2025-54093 Windows TCP/IP Driver Elevation of Privilege Vulnerability
- CVE-2025-54092 Windows Hyper-V Elevation of Privilege Vulnerability
- CVE-2025-54091 Windows Hyper-V Elevation of Privilege Vulnerability
- CVE-2025-53810 Windows Defender Firewall Service Elevation of Privilege Vulnerability
- CVE-2025-53809 Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability
- CVE-2025-53808 Windows Defender Firewall Service Elevation of Privilege Vulnerability
- CVE-2025-53807 Windows Graphics Component Elevation of Privilege Vulnerability
- CVE-2025-53806 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-53805 HTTP.sys Denial of Service Vulnerability
- CVE-2025-53804 Windows Kernel-Mode Driver Information Disclosure Vulnerability
- CVE-2025-53803 Windows Kernel Memory Information Disclosure Vulnerability
- CVE-2025-53802 Windows Bluetooth Service Elevation of Privilege Vulnerability
- CVE-2025-53801 Microsoft DWM Core Library Elevation of Privilege Vulnerability
- CVE-2025-53800 Windows Graphics Component Elevation of Privilege Vulnerability
- CVE-2025-53799 Windows Imaging Component Information Disclosure Vulnerability
- CVE-2025-53798 Windows Routing and Remote Access Service (RRAS) Information

Disclosure Vulnerability

- CVE-2025-53797 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-53796 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-49734 PowerShell Direct 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	KB5065428	windows10.0-kb5065428-x64_3c83399a5ec7b56767218da3a1823e6349ceafb1.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5065428	windows10.0-kb5065428-x64_3c83399a5ec7b56767218da3a1823e6349ceafb1.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5065427	windows10.0-kb5065427-x86_4ff5e11c8c3a43b93abbf014dfabdf8945655843.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5065427	windows10.0-kb5065427-x64_b341c6fc803e28fc7257524e5f5de44551766bcf.msu	KB4498947 KB4132216
	Windows Server 2016	KB5065427	windows10.0-kb5065427-x64_b341c6fc803e28fc7257524e5f5de44551766bcf.msu	KB4498947 KB4132216
BeneVision CMS Viewer	Windows 10 Professional SP1 64bit 1809	KB5065428	windows10.0-kb5065428-x64_3c83399a5ec7b56767218da3a1823e6349ceafb1.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5065427	windows10.0-kb5065427-x86_4ff5e11c8c3a43b93abbf014dfabdf8945655843.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5065427	windows10.0-kb5065427-x64_b341c6fc803e28fc7257524e5f5de44551766bcf.msu	KB4498947 KB4132216
Hypervisor X CMS	Windows 10 Professional SP1 64bit 1809	KB5065428	windows10.0-kb5065428-x64_3c83399a5ec7b56767218da3a1823e6349ceafb1.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5065428	windows10.0-kb5065428-x64_3c83399a5ec7b56767218da3a1823e6349ceafb1.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5065427	windows10.0-kb5065427-x86_4ff5e11c8c3a43b93abbf014dfabdf8945655843.msu	KB4498947 KB4132216

	Windows 10 1607 for x64-based	KB5065427	windows10.0-kb5065427-x64_b341c6fc803e28fc7257524e5f5de44551766bcf.msu	KB4498947 KB4132216
eGateway	Windows 10 Professional SP1 64bit 1809	KB5065428	windows10.0-kb5065428-x64_3c83399a5ec7b56767218da3a1823e6349ceafb1.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5065428	windows10.0-kb5065428-x64_3c83399a5ec7b56767218da3a1823e6349ceafb1.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for x64-based	KB5065427	windows10.0-kb5065427-x64_b341c6fc803e28fc7257524e5f5de44551766bcf.msu	KB4498947 KB4132216
	Windows Server 2016	KB5065427	windows10.0-kb5065427-x64_b341c6fc803e28fc7257524e5f5de44551766bcf.msu	KB4498947 KB4132216
MLDAP Server	Windows 10 1607 for x64-based	KB5065427	windows10.0-kb5065427-x64_b341c6fc803e28fc7257524e5f5de44551766bcf.msu	KB4498947 KB4132216
	Windows Server 2016	KB5065427	windows10.0-kb5065427-x64_b341c6fc803e28fc7257524e5f5de44551766bcf.msu	KB4498947 KB4132216
	Windows Server 2019	KB5065428	windows10.0-kb5065428-x64_3c83399a5ec7b56767218da3a1823e6349ceafb1.msu	KB5005112 KB5003243 KB4587735
BeneVision Mobile Server	Windows Server 2016	KB5065427	windows10.0-kb5065427-x64_b341c6fc803e28fc7257524e5f5de44551766bcf.msu	KB4498947 KB4132216
	Windows Server 2019	KB5065428	windows10.0-kb5065428-x64_3c83399a5ec7b56767218da3a1823e6349ceafb1.msu	KB5005112 KB5003243 KB4587735
iView	Windows 10 1607 for x64-based	KB5065427	windows10.0-kb5065427-x64_b341c6fc803e28fc7257524e5f5de44551766bcf.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：2025-9-28