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

## CVE Identifiers

- CVE-2025-59502 Remote Procedure Call Denial of Service Vulnerability
- CVE-2025-59295 Windows URL Parsing Remote Code Execution Vulnerability
- CVE-2025-59294 Windows Taskbar Live Preview Information Disclosure Vulnerability
- CVE-2025-59290 Windows Bluetooth Service Elevation of Privilege Vulnerability
- CVE-2025-59289 Windows Bluetooth Service Elevation of Privilege Vulnerability
- CVE-2025-59287 Windows Server Update Service (WSUS) Remote Code Execution Vulnerability
- CVE-2025-59284 Windows NTLM Spoofing Vulnerability
- CVE-2025-59282 Internet Information Services (IIS) Inbox COM Objects (Global Memory) Remote Code Execution Vulnerability
- CVE-2025-59280 Windows SMB Client Tampering Vulnerability
- CVE-2025-59278 Windows Authentication Elevation of Privilege Vulnerability
- CVE-2025-59277 Windows Authentication Elevation of Privilege Vulnerability
- CVE-2025-59275 Windows Authentication Elevation of Privilege Vulnerability
- CVE-2025-59261 Windows Graphics Component Elevation of Privilege Vulnerability
- CVE-2025-59260 Microsoft Failover Cluster Virtual Driver Information Disclosure Vulnerability
- CVE-2025-59259 Windows Local Session Manager (LSM) Denial of Service Vulnerability
- CVE-2025-59258 Windows Active Directory Federation Services (ADFS) Information Disclosure Vulnerability
- CVE-2025-59257 Windows Local Session Manager (LSM) Denial of Service Vulnerability
- CVE-2025-59255 Windows DWM Core Library Elevation of Privilege Vulnerability
- CVE-2025-59254 Microsoft DWM Core Library Elevation of Privilege Vulnerability
- CVE-2025-59253 Windows Search Service Denial of Service Vulnerability
- CVE-2025-59244 NTLM Hash Disclosure Spoofing Vulnerability
- CVE-2025-59242 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
- CVE-2025-59241 Windows Health and Optimized Experiences Elevation of Privilege Vulnerability
- CVE-2025-59230 Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
- CVE-2025-59214 Microsoft Windows File Explorer Spoofing Vulnerability

- CVE-2025-59211 Windows Push Notification Information Disclosure Vulnerability
- CVE-2025-59210 Windows Resilient File System (ReFS) Deduplication Service Elevation of Privilege Vulnerability
- CVE-2025-59209 Windows Push Notification Information Disclosure Vulnerability
- CVE-2025-59208 Windows MapUrlToZone Information Disclosure Vulnerability
- CVE-2025-59207 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2025-59206 Windows Resilient File System (ReFS) Deduplication Service Elevation of Privilege Vulnerability
- CVE-2025-59205 Windows Graphics Component Elevation of Privilege Vulnerability
- CVE-2025-59204 Windows Management Services Information Disclosure Vulnerability
- CVE-2025-59203 Windows State Repository API Server File Information Disclosure Vulnerability
- CVE-2025-59202 Windows Remote Desktop Services Elevation of Privilege Vulnerability
- CVE-2025-59201 Network Connection Status Indicator (NCSI) Elevation of Privilege Vulnerability
- CVE-2025-59200 Data Sharing Service Spoofing Vulnerability
- CVE-2025-59199 Software Protection Platform (SPP) Elevation of Privilege Vulnerability
- CVE-2025-59198 Windows Search Service Denial of Service Vulnerability
- CVE-2025-59197 Windows ETL Channel Information Disclosure Vulnerability
- CVE-2025-59196 Windows Simple Search and Discovery Protocol (SSDP) Service Elevation of Privilege Vulnerability
- CVE-2025-59195 Microsoft Graphics Component Denial of Service Vulnerability
- CVE-2025-59194 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2025-59193 Windows Management Services Elevation of Privilege Vulnerability
- CVE-2025-59192 Storport.sys Driver Elevation of Privilege Vulnerability
- CVE-2025-59191 Windows Connected Devices Platform Service Elevation of Privilege Vulnerability
- CVE-2025-59190 Windows Search Service Denial of Service Vulnerability
- CVE-2025-59189 Microsoft Brokering File System Elevation of Privilege Vulnerability
- CVE-2025-59188 Microsoft Failover Cluster Information Disclosure Vulnerability
- CVE-2025-59187 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2025-59186 Windows Kernel Information Disclosure Vulnerability
- CVE-2025-59185 NTLM Hash Disclosure Spoofing Vulnerability
- CVE-2025-59184 Storage Spaces Direct Information Disclosure Vulnerability
- CVE-2025-58739 Microsoft Windows File Explorer Spoofing Vulnerability
- CVE-2025-58738 Inbox COM Objects (Global Memory) Remote Code Execution Vulnerability
- CVE-2025-58737 Remote Desktop Protocol Remote Code Execution Vulnerability
- CVE-2025-58736 Inbox COM Objects (Global Memory) Remote Code Execution Vulnerability
- CVE-2025-58735 Inbox COM Objects (Global Memory) Remote Code Execution Vulnerability
- CVE-2025-58734 Inbox COM Objects (Global Memory) Remote Code Execution Vulnerability
- CVE-2025-58733 Inbox COM Objects (Global Memory) Remote Code Execution

Vulnerability
- CVE-2025-58732 Inbox COM Objects (Global Memory) Remote Code Execution Vulnerability
- CVE-2025-58731 Inbox COM Objects (Global Memory) Remote Code Execution Vulnerability
- CVE-2025-58730 Inbox COM Objects (Global Memory) Remote Code Execution Vulnerability
- CVE-2025-58729 Windows Local Session Manager (LSM) Denial of Service Vulnerability
- CVE-2025-58728 Windows Bluetooth Service Elevation of Privilege Vulnerability
- CVE-2025-58727 Windows Connected Devices Platform Service Elevation of Privilege Vulnerability
- CVE-2025-58726 Windows SMB Server Elevation of Privilege Vulnerability
- CVE-2025-58725 Windows COM+ Event System Service Elevation of Privilege Vulnerability
- CVE-2025-58722 Microsoft DWM Core Library Elevation of Privilege Vulnerability
- CVE-2025-58720 Windows Cryptographic Services Information Disclosure Vulnerability
- CVE-2025-58719 Windows Connected Devices Platform Service Elevation of Privilege Vulnerability
- CVE-2025-58718 Remote Desktop Client Remote Code Execution Vulnerability
- CVE-2025-58717 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-58716 Windows Speech Runtime Elevation of Privilege Vulnerability
- CVE-2025-58715 Windows Speech Runtime Elevation of Privilege Vulnerability
- CVE-2025-58714 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
- CVE-2025-55701 Windows Authentication Elevation of Privilege Vulnerability
- CVE-2025-55700 Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability
- CVE-2025-55699 Windows Kernel Information Disclosure Vulnerability
- CVE-2025-55698 DirectX Graphics Kernel Denial of Service Vulnerability
- CVE-2025-55696 NtQueryInformation Token function (ntifs.h) Elevation of Privilege Vulnerability
- CVE-2025-55695 Windows WLAN AutoConfig Service Information Disclosure Vulnerability
- CVE-2025-55694 Windows Error Reporting Service Elevation of Privilege Vulnerability
- CVE-2025-55693 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2025-55692 Windows Error Reporting Service Elevation of Privilege Vulnerability
- CVE-2025-55691 Windows PrintWorkflowUserSvc Elevation of Privilege Vulnerability
- CVE-2025-55690 Windows PrintWorkflowUserSvc Elevation of Privilege Vulnerability
- CVE-2025-55689 Windows PrintWorkflowUserSvc Elevation of Privilege Vulnerability
- CVE-2025-55688 Windows PrintWorkflowUserSvc Elevation of Privilege Vulnerability
- CVE-2025-55687 Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability
- CVE-2025-55686 Windows PrintWorkflowUserSvc Elevation of Privilege Vulnerability

- CVE-2025-55685 Windows PrintWorkflowUserSvc Elevation of Privilege Vulnerability
- CVE-2025-55684 Windows PrintWorkflowUserSvc Elevation of Privilege Vulnerability
- CVE-2025-55683 Windows Kernel Information Disclosure Vulnerability
- CVE-2025-55682 Windows BitLocker Security Feature Bypass Vulnerability
- CVE-2025-55681 Desktop Windows Manager Elevation of Privilege Vulnerability
- CVE-2025-55680 Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
- CVE-2025-55679 Windows Kernel Information Disclosure Vulnerability
- CVE-2025-55678 DirectX Graphics Kernel Elevation of Privilege Vulnerability
- CVE-2025-55677 Windows Device Association Broker Service Elevation of Privilege Vulnerability
- CVE-2025-55676 Windows USB Video Class System Driver Information Disclosure Vulnerability
- CVE-2025-55340 Windows Remote Desktop Protocol Security Feature Bypass
- CVE-2025-55339 Windows Network Driver Interface Specification Driver Elevation of Privilege Vulnerability
- CVE-2025-55338 Windows BitLocker Security Feature Bypass Vulnerability
- CVE-2025-55337 Windows BitLocker Security Feature Bypass Vulnerability
- CVE-2025-55336 Windows Cloud Files Mini Filter Driver Information Disclosure Vulnerability
- CVE-2025-55335 Windows NTFS Elevation of Privilege Vulnerability
- CVE-2025-55334 Windows Kernel Security Feature Bypass Vulnerability
- CVE-2025-55333 Windows BitLocker Security Feature Bypass Vulnerability
- CVE-2025-55332 Windows BitLocker Security Feature Bypass Vulnerability
- CVE-2025-55331 Windows PrintWorkflowUserSvc Elevation of Privilege Vulnerability
- CVE-2025-55330 Windows BitLocker Security Feature Bypass Vulnerability
- CVE-2025-55328 Windows Hyper-V Elevation of Privilege Vulnerability
- CVE-2025-55326 Windows Connected Devices Platform Service (Cdpsvc) Remote Code Execution Vulnerability
- CVE-2025-55325 Windows Storage Management Provider Information Disclosure Vulnerability
- CVE-2025-54957 MITRE CVE-2025-54957: Integer overflow in Dolby Digital Plus audio decoder
- CVE-2025-53768 Xbox IStorageService Elevation of Privilege Vulnerability
- CVE-2025-53717 Windows Virtualization-Based Security (VBS) Enclave Elevation of Privilege Vulnerability
- CVE-2025-53150 Windows Digital Media Elevation of Privilege Vulnerability
- CVE-2025-53139 Windows Hello Security Feature Bypass Vulnerability
- CVE-2025-50175 Windows Digital Media Elevation of Privilege Vulnerability
- CVE-2025-50174 Windows Device Association Broker Service Elevation of Privilege Vulnerability
- CVE-2025-49708 Microsoft Graphics Component Elevation of Privilege Vulnerability
- CVE-2025-48813 Virtual Secure Mode Spoofing Vulnerability
- CVE-2025-48004 Microsoft Brokering File System Elevation of Privilege Vulnerability
- CVE-2025-47827 MITRE CVE-2025-47827: Secure Boot bypass in IGEL OS before 11
- CVE-2025-2884 Cert CC: CVE-2025-2884 Out-of-Bounds read vulnerability in TCG TPM2.0 reference implementation

- CVE-2025-25004 PowerShell Elevation of Privilege Vulnerability
- CVE-2025-24990 Windows Agere Modem Driver Elevation of Privilege Vulnerability
- CVE-2025-24052 Windows Agere Modem Driver Elevation of Privilege Vulnerability
- CVE-2016-9535 MITRE CVE-2016-9535: LibTIFF Heap Buffer Overflow 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 | KB5066586 | windows10.0-kb5066586-x64_062fcc3be6982521409b3c7021f8c99b9975eb18.msu | KB5005112 KB5003243 KB4587735 |
| | Windows Server 2019 | KB5066586 | windows10.0-kb5066586-x64_062fcc3be6982521409b3c7021f8c99b9975eb18.msu | KB5005112 KB5003243 KB4587735 |
| | Windows 10 1607 for 32-bit | KB5066836 | windows10.0-kb5066836-x86_06fd6e0daf2d58400e107a16cab525884f1865ea.msu | KB4498947 KB4132216 |
| | Windows 10 1607 for x64-based | KB5066836 | windows10.0-kb5066836-x64_f190747df5cdd3a136cbcfae8331b37fba306baf.msu | KB4498947 KB4132216 |
| | Windows Server 2016 | KB5066836 | windows10.0-kb5066836-x64_f190747df5cdd3a136cbcfae8331b37fba306baf.msu | KB4498947 KB4132216 |
| BeneVision CMS Viewer | Windows 10 Professional SP1 64bit 1809 | KB5066586 | windows10.0-kb5066586-x64_062fcc3be6982521409b3c7021f8c99b9975eb18.msu | KB5005112 KB5003243 KB4587735 |
| | Windows 10 1607 for 32-bit | KB5066836 | windows10.0-kb5066836-x86_06fd6e0daf2d58400e107a16cab525884f1865ea.msu | KB4498947 KB4132216 |
| | Windows 10 1607 for x64-based | KB5066836 | windows10.0-kb5066836-x64_f190747df5cdd3a136cbcfae8331b37fba306baf.msu | KB4498947 KB4132216 |
| Hypervisor X CMS | Windows 10 Professional SP1 64bit 1809 | KB5066586 | windows10.0-kb5066586-x64_062fcc3be6982521409b3c7021f8c99b9975eb18.msu | KB5005112 KB5003243 KB4587735 |
| | Windows Server 2019 | KB5066586 | windows10.0-kb5066586-x64_062fcc3be6982521409b3c7021f8c99b9975eb18.msu | KB5005112 KB5003243 KB4587735 |
| | Windows 10 1607 for 32-bit | KB5066836 | windows10.0-kb5066836-x86_06fd6e0daf2d58400e107a16cab525884f1865ea.msu | KB4498947 KB4132216 |
| | Windows 10 1607 for x64- | KB5066836 | windows10.0-kb5066836-x64_f190747df5cdd3a136cbcfae8331b37fba306baf.msu | KB4498947 KB4132216 |

| | | | | |
|---|---|---|---|---|
| | based | | | |
| eGateway | Windows 10 Professional SP1 64bit 1809 | KB5066586 | windows10.0-kb5066586-x64_062fcc3be6982521409b3c7021f8c99b9975eb18.msu | KB5005112<br>KB5003243<br>KB4587735 |
| | Windows Server 2019 | KB5066586 | windows10.0-kb5066586-x64_062fcc3be6982521409b3c7021f8c99b9975eb18.msu | KB5005112<br>KB5003243<br>KB4587735 |
| | Windows 10 1607 for x64-based | KB5066836 | windows10.0-kb5066836-x64_f190747df5cdd3a136cbcfae8331b37fba306baf.msu | KB4498947<br>KB4132216 |
| | Windows Server 2016 | KB5066836 | windows10.0-kb5066836-x64_f190747df5cdd3a136cbcfae8331b37fba306baf.msu | KB4498947<br>KB4132216 |
| MLDAP Server | Windows 10 1607 for x64-based | KB5066836 | windows10.0-kb5066836-x64_f190747df5cdd3a136cbcfae8331b37fba306baf.msu | KB4498947<br>KB4132216 |
| | Windows Server 2016 | KB5066836 | windows10.0-kb5066836-x64_f190747df5cdd3a136cbcfae8331b37fba306baf.msu | KB4498947<br>KB4132216 |
| | Windows Server 2019 | KB5066586 | windows10.0-kb5066586-x64_062fcc3be6982521409b3c7021f8c99b9975eb18.msu | KB5005112<br>KB5003243<br>KB4587735 |
| BeneVision Mobile Server | Windows Server 2016 | KB5066836 | windows10.0-kb5066836-x64_f190747df5cdd3a136cbcfae8331b37fba306baf.msu | KB4498947<br>KB4132216 |
| | Windows Server 2019 | KB5066586 | windows10.0-kb5066586-x64_062fcc3be6982521409b3c7021f8c99b9975eb18.msu | KB5005112<br>KB5003243<br>KB4587735 |
| iView | Windows 10 1607 for x64-based | KB5066836 | windows10.0-kb5066836-x64_f190747df5cdd3a136cbcfae8331b37fba306baf.msu | KB4498947<br>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.