Security Patches for Mindray Products Running on Windows OS (April, 2026)

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, 2026. The following CVEs have been evaluated:

CVE Identifiers

- CVE-2026-33829 Windows Snipping Tool Spoofing Vulnerability
- CVE-2026-33827 Windows TCP/IP Remote Code Execution Vulnerability
- CVE-2026-33826 Windows Active Directory Remote Code Execution Vulnerability
- CVE-2026-33824 Windows Internet Key Exchange (IKE) Service Extensions Remote Code Execution Vulnerability
- CVE-2026-33104 Win32k Elevation of Privilege Vulnerability
- CVE-2026-33100 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
- CVE-2026-33099 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
- CVE-2026-33098 Windows Container Isolation FS Filter Driver Elevation of Privilege Vulnerability
- CVE-2026-32225 Windows Shell Security Feature Bypass Vulnerability
- CVE-2026-32217 Windows Kernel Information Disclosure Vulnerability
- CVE-2026-32215 Windows Kernel Information Disclosure Vulnerability
- CVE-2026-32214 Universal Plug and Play (upnp.dll) Information Disclosure Vulnerability
- CVE-2026-32212 Universal Plug and Play (upnp.dll) Information Disclosure Vulnerability
- CVE-2026-32183 Windows Snipping Tool Remote Code Execution Vulnerability
- CVE-2026-32165 Windows User Interface Core Elevation of Privilege Vulnerability
- CVE-2026-32164 Windows User Interface Core Elevation of Privilege Vulnerability
- CVE-2026-32163 Windows User Interface Core Elevation of Privilege Vulnerability
- CVE-2026-32162 Windows COM Elevation of Privilege Vulnerability
- CVE-2026-32160 Windows Push Notifications Elevation of Privilege Vulnerability
- CVE-2026-32159 Windows Push Notifications Elevation of Privilege Vulnerability
- CVE-2026-32158 Windows Push Notifications Elevation of Privilege Vulnerability
- CVE-2026-32157 Remote Desktop Client Remote Code Execution Vulnerability
- CVE-2026-32156 Windows UPnP Device Host Remote Code Execution Vulnerability
- CVE-2026-32154 Desktop Window Manager Elevation of Privilege Vulnerability
- CVE-2026-32153 Windows Speech Runtime Elevation of Privilege Vulnerability
- CVE-2026-32151 Windows Shell Information Disclosure Vulnerability
- CVE-2026-32150 Windows Function Discovery Service (fdwsd.dll) Elevation of Privilege Vulnerability

- CVE-2026-32149 Windows Hyper-V Remote Code Execution Vulnerability
- CVE-2026-32093 Windows Function Discovery Service (fdwsd.dll) Elevation of Privilege Vulnerability
- CVE-2026-32091 Microsoft Brokering File System Elevation of Privilege Vulnerability
- CVE-2026-32090 Windows Speech Brokered Api Elevation of Privilege Vulnerability
- CVE-2026-32089 Windows Speech Brokered Api Elevation of Privilege Vulnerability
- CVE-2026-32088 Windows Biometric Service Security Feature Bypass Vulnerability
- CVE-2026-32087 Windows Function Discovery Service (fdwsd.dll) Elevation of Privilege Vulnerability
- CVE-2026-32086 Windows Function Discovery Service (fdwsd.dll) Elevation of Privilege Vulnerability
- CVE-2026-32085 Remote Procedure Call Information Disclosure Vulnerability
- CVE-2026-32084 Windows Print Spooler Information Disclosure Vulnerability
- CVE-2026-32083 Windows Simple Search and Discovery Protocol (SSDP) Service Elevation of Privilege Vulnerability
- CVE-2026-32082 Windows Simple Search and Discovery Protocol (SSDP) Service Elevation of Privilege Vulnerability
- CVE-2026-32081 Package Catalog Information Disclosure Vulnerability
- CVE-2026-32080 Windows WalletService Elevation of Privilege Vulnerability
- CVE-2026-32079 Web Account Manager Information Disclosure Vulnerability
- CVE-2026-32078 Windows Projected File System Elevation of Privilege Vulnerability
- CVE-2026-32077 Windows UPnP Device Host Elevation of Privilege Vulnerability
- CVE-2026-32075 Windows UPnP Device Host Elevation of Privilege Vulnerability
- CVE-2026-32074 Windows Projected File System Elevation of Privilege Vulnerability
- CVE-2026-32073 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
- CVE-2026-32072 Active Directory Spoofing Vulnerability
- CVE-2026-32071 Windows Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability
- CVE-2026-32070 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2026-32069 Windows Projected File System Elevation of Privilege Vulnerability
- CVE-2026-32068 Windows Simple Search and Discovery Protocol (SSDP) Service Elevation of Privilege Vulnerability
- CVE-2026-27930 Windows GDI Information Disclosure Vulnerability
- CVE-2026-27929 Windows LUA File Virtualization Filter Driver Elevation of Privilege Vulnerability
- CVE-2026-27928 Windows Hello Security Feature Bypass Vulnerability
- CVE-2026-27927 Windows Projected File System Elevation of Privilege Vulnerability
- CVE-2026-27926 Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
- CVE-2026-27925 Windows UPnP Device Host Information Disclosure Vulnerability
- CVE-2026-27923 Desktop Window Manager Elevation of Privilege Vulnerability
- CVE-2026-27922 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
- CVE-2026-27921 Windows TDI Translation Driver (tdx.sys) Elevation of Privilege Vulnerability
- CVE-2026-27920 Windows UPnP Device Host Elevation of Privilege Vulnerability

- CVE-2026-27919 Windows UPnP Device Host Elevation of Privilege Vulnerability
- CVE-2026-27918 Windows Shell Elevation of Privilege Vulnerability
- CVE-2026-27917 Windows WFP NDIS Lightweight Filter Driver (wfplwfs.sys) Elevation of Privilege Vulnerability
- CVE-2026-27916 Windows UPnP Device Host Elevation of Privilege Vulnerability
- CVE-2026-27915 Windows UPnP Device Host Elevation of Privilege Vulnerability
- CVE-2026-27914 Microsoft Management Console Elevation of Privilege Vulnerability
- CVE-2026-27913 Windows BitLocker Security Feature Bypass Vulnerability
- CVE-2026-27912 Windows Kerberos Elevation of Privilege Vulnerability
- CVE-2026-27911 Windows User Interface Core Elevation of Privilege Vulnerability
- CVE-2026-27910 Windows Installer Elevation of Privilege Vulnerability
- CVE-2026-27909 Windows Search Service Elevation of Privilege Vulnerability
- CVE-2026-27908 Windows TDI Translation Driver (tdx.sys) Elevation of Privilege Vulnerability
- CVE-2026-26184 Windows Projected File System Elevation of Privilege Vulnerability
- CVE-2026-26183 Remote Access Management service/API (RPC server) Elevation of Privilege Vulnerability
- CVE-2026-26182 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
- CVE-2026-26180 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2026-26179 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2026-26178 Windows Advanced Rasterization Platform Elevation of Privilege Vulnerability
- CVE-2026-26177 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
- CVE-2026-26176 Windows Client Side Caching driver (csc.sys) Elevation of Privilege Vulnerability
- CVE-2026-26175 Windows Boot Manager Security Feature Bypass Vulnerability
- CVE-2026-26174 Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability
- CVE-2026-26173 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
- CVE-2026-26170 PowerShell Elevation of Privilege Vulnerability
- CVE-2026-26169 Windows Kernel Memory Information Disclosure Vulnerability
- CVE-2026-26168 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
- CVE-2026-26167 Windows Push Notifications Elevation of Privilege Vulnerability
- CVE-2026-26163 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2026-26162 Windows OLE Elevation of Privilege Vulnerability
- CVE-2026-26161 Windows Sensor Data Service Elevation of Privilege Vulnerability
- CVE-2026-26160 Remote Desktop Licensing Service Elevation of Privilege Vulnerability
- CVE-2026-26159 Remote Desktop Licensing Service Elevation of Privilege Vulnerability
- CVE-2026-26156 Windows Hyper-V Remote Code Execution Vulnerability
- CVE-2026-26155 Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability
- CVE-2026-26154 Windows Server Update Service (WSUS) Tampering Vulnerability

- CVE-2026-26153 Windows Encrypted File System (EFS) Elevation of Privilege Vulnerability
- CVE-2026-26152 Microsoft Cryptographic Services Elevation of Privilege Vulnerability
- CVE-2026-26151 Remote Desktop Spoofing Vulnerability
- CVE-2026-23670 Windows Virtualization-Based Security (VBS) Security Feature Bypass Vulnerability
- CVE-2026-20930 Windows Management Services Elevation of Privilege Vulnerability
- CVE-2026-20928 Windows Recovery Environment Security Feature Bypass Vulnerability
- CVE-2026-20806 Windows COM Server Information Disclosure Vulnerability
- CVE-2026-0390 UEFI Secure Boot Security Feature Bypass 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 1607 for x64-based	KB5082198	windows10.0-kb5082198-x64_2f64ef5389462c14d458858ba6a098d9b4e2a63a.msu	KB5070247 KB5050109 KB4498947 KB4132216
	Windows 10 1607 for 32-bit	KB5082198	windows10.0-kb5082198-x86_98d93f430dc6a89a6c6ab18e4212526d5497fa9e.msu	KB5070247 KB5050109 KB4498947 KB4132216
	Windows 10 Professional SP1 64bit 1809	KB5082123	windows10.0-kb5082123-x64_3c1a2626005bdced0829822c5329ca30519d083c.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2016	KB5082198	windows10.0-kb5082198-x64_2f64ef5389462c14d458858ba6a098d9b4e2a63a.msu	KB5070247 KB5050109 KB4498947 KB4132216
	Windows Server 2019	KB5082123	windows10.0-kb5082123-x64_3c1a2626005bdced0829822c5329ca30519d083c.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2022	KB5082142	windows10.0-kb5082142-x64_0d2677e2b8f6550a978bd89e8991c4d3813ccf1f.msu	/
BeneVision CMS Viewer	Windows 10 Professional SP1 64bit 1809	KB5082123	windows10.0-kb5082123-x64_3c1a2626005bdced0829822c5329ca30519d083c.msu	KB5005112 KB5003243 KB4587735

	Windows 10 1607 for 32-bit	KB5082198	windows10.0-kb5082198-x86_98d93f430dc6a89a6c6ab18e4212526d5497fa9e.msu	KB5070247 KB5050109 KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5082198	windows10.0-kb5082198-x64_2f64ef5389462c14d458858ba6a098d9b4e2a63a.msu	KB5070247 KB5050109 KB4498947 KB4132216
Hypervisor X CMS	Windows 10 Professional SP1 64bit 1809	KB5082123	windows10.0-kb5082123-x64_3c1a2626005bdced0829822c5329ca30519d083c.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5082123	windows10.0-kb5082123-x64_3c1a2626005bdced0829822c5329ca30519d083c.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5082198	windows10.0-kb5082198-x86_98d93f430dc6a89a6c6ab18e4212526d5497fa9e.msu	KB5070247 KB5050109 KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5082198	windows10.0-kb5082198-x64_2f64ef5389462c14d458858ba6a098d9b4e2a63a.msu	KB5070247 KB5050109 KB4498947 KB4132216
eGateway	Windows 10 Professional SP1 64bit 1809	KB5078752	windows10.0-kb5078752-x64_d19dce98bd2132ac8dcf4ae644ff36ec1ac7a734.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5078752	windows10.0-kb5078752-x64_d19dce98bd2132ac8dcf4ae644ff36ec1ac7a734.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for x64-based	KB5078938	windows10.0-kb5078938-x64_4f2644d71dfb3459b6777dfb1a3a4e16cf3877f5.msu	KB5070247 KB5050109 KB4498947 KB4132216
	Windows Server 2016	KB5078938	windows10.0-kb5078938-x64_4f2644d71dfb3459b6777dfb1a3a4e16cf3877f5.msu	KB5070247 KB5050109 KB4498947 KB4132216
MLDAP Server	Windows 10 1607 for x64-based	KB5078938	windows10.0-kb5078938-x64_4f2644d71dfb3459b6777dfb1a3a4e16cf3877f5.msu	KB5070247 KB5050109 KB4498947 KB4132216
	Windows Server 2016	KB5078938	windows10.0-kb5078938-x64_4f2644d71dfb3459b6777dfb1a3a4e16cf3877f5.msu	KB5070247 KB5050109 KB4498947 KB4132216
	Windows Server 2019	KB5078752	windows10.0-kb5078752-x64_d19dce98bd2132ac8dcf4ae644ff36ec1ac7a734.msu	KB5005112 KB5003243 KB4587735

BeneVision Mobile Server	Windows Server 2016	KB5078938	windows10.0-kb5078938-x64_4f2644d71dfb3459b6777dfb1a3a4e16cf3877f5.msu	KB5070247 KB5050109 KB4498947 KB4132216
	Windows Server 2019	KB5078752	windows10.0-kb5078752-x64_d19dce98bd2132ac8dcf4ae644ff36ec1ac7a734.msu	KB5005112 KB5003243 KB4587735
iView (N series)	Windows 10 1607 for x64-based	KB5078938	windows10.0-kb5078938-x64_4f2644d71dfb3459b6777dfb1a3a4e16cf3877f5.msu	KB5070247 KB5050109 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：2026-05-08