Security Patches for Mindray Products Running on Windows OS (July, 2023)

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, 2023. The following CVEs have been evaluated:

CVE Identifiers

- CVE-2023-36884 Office and Windows HTML Remote Code Execution Vulnerability
- CVE-2023-36874 Windows Error Reporting Service Elevation of Privilege Vulnerability
- CVE-2023-36871 Azure Active Directory Security Feature Bypass Vulnerability
- CVE-2023-35367 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
- CVE-2023-35366 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
- CVE-2023-35365 Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability
- CVE-2023-35364 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-35363 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-35362 Windows Clip Service Elevation of Privilege Vulnerability
- CVE-2023-35361 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-35360 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-35358 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-35357 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-35356 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-35353 Connected User Experiences and Telemetry Elevation of Privilege Vulnerability
- CVE-2023-35352 Windows Remote Desktop Security Feature Bypass Vulnerability
- CVE-2023-35351 Windows Active Directory Certificate Services (AD CS) Remote Code Execution Vulnerability
- CVE-2023-35350 Windows Active Directory Certificate Services (AD CS) Remote Code Execution Vulnerability
- CVE-2023-35348 Active Directory Federation Service Security Feature Bypass Vulnerability
- CVE-2023-35346 Windows DNS Server Remote Code Execution Vulnerability
- CVE-2023-35345 Windows DNS Server Remote Code Execution Vulnerability
- CVE-2023-35344 Windows DNS Server Remote Code Execution Vulnerability
- CVE-2023-35343 Windows Geolocation Service Remote Code Execution Vulnerability
- CVE-2023-35342 Windows Image Acquisition Elevation of Privilege Vulnerability
- CVE-2023-35341 Microsoft DirectMusic Information Disclosure Vulnerability
- CVE-2023-35340 Windows CNG Key Isolation Service Elevation of Privilege Vulnerability

- CVE-2023-35339 Windows CryptoAPI Denial of Service Vulnerability
- CVE-2023-35338 Windows Peer Name Resolution Protocol Denial of Service Vulnerability
- CVE-2023-35336 Windows MSHTML Platform Security Feature Bypass Vulnerability
- CVE-2023-35332 Windows Remote Desktop Protocol Security Feature Bypass
- CVE-2023-35331 Windows Local Security Authority (LSA) Denial of Service Vulnerability
- CVE-2023-35330 Windows Extended Negotiation Denial of Service Vulnerability
- CVE-2023-35329 Windows Authentication Denial of Service Vulnerability
- CVE-2023-35328 Windows Transaction Manager Elevation of Privilege Vulnerability
- CVE-2023-35326 Windows CDP User Components Information Disclosure Vulnerability
- CVE-2023-35325 Windows Print Spooler Information Disclosure Vulnerability
- CVE-2023-35324 Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
- CVE-2023-35322 Windows Deployment Services Remote Code Execution Vulnerability
- CVE-2023-35321 Windows Deployment Services Denial of Service Vulnerability
- CVE-2023-35320 Connected User Experiences and Telemetry Elevation of Privilege Vulnerability
- CVE-2023-35319 Remote Procedure Call Runtime Denial of Service Vulnerability
- CVE-2023-35318 Remote Procedure Call Runtime Denial of Service Vulnerability
- CVE-2023-35317 Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability
- CVE-2023-35316 Remote Procedure Call Runtime Information Disclosure Vulnerability
- CVE-2023-35315 Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability
- CVE-2023-35314 Remote Procedure Call Runtime Denial of Service Vulnerability
- CVE-2023-35313 Windows Online Certificate Status Protocol (OCSP) SnapIn Remote Code Execution Vulnerability
- CVE-2023-35311 Microsoft Outlook Security Feature Bypass Vulnerability
- CVE-2023-35310 Windows DNS Server Remote Code Execution Vulnerability
- CVE-2023-35309 Microsoft Message Queuing Remote Code Execution Vulnerability
- CVE-2023-35308 Windows MSHTML Platform Security Feature Bypass Vulnerability
- CVE-2023-35306 Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
- CVE-2023-35305 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-35304 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-35303 USB Audio Class System Driver Remote Code Execution Vulnerability
- CVE-2023-35302 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
- CVE-2023-35300 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2023-35299 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2023-35297 Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability

- CVE-2023-35296 Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
- CVE-2023-33174 Windows Cryptographic Information Disclosure Vulnerability
- CVE-2023-33173 Remote Procedure Call Runtime Denial of Service Vulnerability
- CVE-2023-33172 Remote Procedure Call Runtime Denial of Service Vulnerability
- CVE-2023-33169 Remote Procedure Call Runtime Denial of Service Vulnerability
- CVE-2023-33168 Remote Procedure Call Runtime Denial of Service Vulnerability
- CVE-2023-33167 Remote Procedure Call Runtime Denial of Service Vulnerability
- CVE-2023-33166 Remote Procedure Call Runtime Denial of Service Vulnerability
- CVE-2023-33164 Remote Procedure Call Runtime Denial of Service Vulnerability
- CVE-2023-33163 Windows Network Load Balancing Remote Code Execution Vulnerability
- CVE-2023-33154 Windows Partition Management Driver Elevation of Privilege Vulnerability
- CVE-2023-32085 Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
- CVE-2023-32084 HTTP.sys Denial of Service Vulnerability
- CVE-2023-32083 Microsoft Failover Cluster Information Disclosure Vulnerability
- CVE-2023-32057 Microsoft Message Queuing Remote Code Execution Vulnerability
- CVE-2023-32056 Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability
- CVE-2023-32055 Active Template Library Elevation of Privilege Vulnerability
- CVE-2023-32054 Volume Shadow Copy Elevation of Privilege Vulnerability
- CVE-2023-32053 Windows Installer Elevation of Privilege Vulnerability
- CVE-2023-32049 Windows SmartScreen Security Feature Bypass Vulnerability
- CVE-2023-32046 Windows MSHTML Platform Elevation of Privilege Vulnerability
- CVE-2023-32045 Microsoft Message Queuing Denial of Service Vulnerability
- CVE-2023-32044 Microsoft Message Queuing Denial of Service Vulnerability
- CVE-2023-32043 Windows Remote Desktop Security Feature Bypass Vulnerability
- CVE-2023-32042 OLE Automation Information Disclosure Vulnerability
- CVE-2023-32041 Windows Update Orchestrator Service Information Disclosure Vulnerability
- CVE-2023-32040 Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
- CVE-2023-32039 Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
- CVE-2023-32038 Microsoft ODBC Driver Remote Code Execution Vulnerability
- CVE-2023-32037 Windows Layer-2 Bridge Network Driver Information Disclosure Vulnerability
- CVE-2023-32035 Remote Procedure Call Runtime Denial of Service Vulnerability
- CVE-2023-32034 Remote Procedure Call Runtime Denial of Service Vulnerability
- CVE-2023-32033 Microsoft Failover Cluster Remote Code Execution Vulnerability
- CVE-2023-21756 Windows Win32k Elevation of Privilege Vulnerability
- CVE-2023-21526 Windows Netlogon Information Disclosure Vulnerability
- ADV230002 Microsoft Guidance for Addressing Security Feature Bypass in Trend Micro EFI Modules
- ADV230001 Guidance on Microsoft Signed Drivers Being Used Maliciously

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	KB5028168	windows10.0-kb5028168-x64_9739e9efd8aafacbd921e14ba1c701da2012464a.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5028168	windows10.0-kb5028168-x64_9739e9efd8aafacbd921e14ba1c701da2012464a.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5028169	windows10.0-kb5028169-x86_8e89c976af39e8317608923d2664bfd7c71c063a.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5028169	windows10.0-kb5028169-x86_8e89c976af39e8317608923d2664bfd7c71c063a.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5028223	windows8.1-kb5028223-x64_1449c6fb5a0ef72a8b8d960127965906104c8142.msu	
	Windows Server 2016	KB5028169	windows10.0-kb5028169-x64_077bf66aff587a4bad99068a77eebd8ee48be55b.msu	KB4498947 KB4132216
BeneVision CMS Viewer	Windows 10 Professional SP1 64bit 1809	KB5028168	windows10.0-kb5028168-x64_9739e9efd8aafacbd921e14ba1c701da2012464a.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5028169	windows10.0-kb5028169-x86_8e89c976af39e8317608923d2664bfd7c71c063a.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5028169	windows10.0-kb5028169-x86_8e89c976af39e8317608923d2664bfd7c71c063a.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5028228	windows8.1-kb5028228-x64_ef910e5284ceb5f65c473564c7cf1a44fcf39c6f.msu	
Hypervisor X CMS	Windows 10 Professional SP1 64bit 1809	KB5028168	windows10.0-kb5028168-x64_9739e9efd8aafacbd921e14ba1c701da2012464a.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5028168	windows10.0-kb5028168-x64_9739e9efd8aafacbd921e14ba1c701da2012464a.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5028169	windows10.0-kb5028169-x86_8e89c976af39e8317608923d2664bfd7c71c063a.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5028169	windows10.0-kb5028169-x86_8e89c976af39e8317608923d2664bfd7c71c063a.msu	KB4498947 KB4132216

eGateway	Windows 10 Professional SP1 64bit 1809	KB5028168	windows10.0-kb5028168-x64_9739e9efd8aafacbd921e14ba1c701da2012464a.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5028168	windows10.0-kb5028168-x64_9739e9efd8aafacbd921e14ba1c701da2012464a.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for x64-based	KB5028169	windows10.0-kb5028169-x86_8e89c976af39e8317608923d2664bfd7c71c063a.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5028223	windows8.1-kb5028223-x64_1449c6fb5a0ef72a8b8d960127965906104c8142.msu	
	Windows Server 2016	KB5028169	windows10.0-kb5028169-x64_077bf66aff587a4bad99068a77eebd8ee48be55b.msu	KB4498947 KB4132216
MLDAP Server	Windows 10 1607 for x64-based	KB5028169	windows10.0-kb5028169-x86_8e89c976af39e8317608923d2664bfd7c71c063a.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5028228	windows8.1-kb5028228-x64_ef910e5284ceb5f65c473564c7cf1a44fcf39c6f.msu	
	Windows Server 2016	KB5028169	windows10.0-kb5028169-x64_077bf66aff587a4bad99068a77eebd8ee48be55b.msu	KB4498947 KB4132216
	Windows Server 2019	KB5028168	windows10.0-kb5028168-x64_9739e9efd8aafacbd921e14ba1c701da2012464a.msu	KB5005112 KB5003243 KB4587735
BeneVision Mobile Server	Windows Server 2016	KB5028169	windows10.0-kb5028169-x64_077bf66aff587a4bad99068a77eebd8ee48be55b.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5028228	windows8.1-kb5028228-x64_ef910e5284ceb5f65c473564c7cf1a44fcf39c6f.msu	
	Windows Server 2019	KB5028168	windows10.0-kb5028168-x64_9739e9efd8aafacbd921e14ba1c701da2012464a.msu	KB5005112 KB5003243 KB4587735
iView	Windows 10 1607 for x64-based	KB5028169	windows10.0-kb5028169-x86_8e89c976af39e8317608923d2664bfd7c71c063a.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：2023-8-15