Security Patches for Mindray Products Running on Windows OS (Oct, 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 Oct, 2023. The following CVEs have been evaluated:

CVE Identifiers

- CVE-2023-44487 MITRE: CVE-2023-44487 HTTP/2 Rapid Reset Attack
- CVE-2023-41774 Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
- CVE-2023-41773 Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
- CVE-2023-41772 Win32k Elevation of Privilege Vulnerability
- CVE-2023-41771 Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
- CVE-2023-41770 Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
- CVE-2023-41769 Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
- CVE-2023-41768 Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
- CVE-2023-41767 Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
- CVE-2023-38166 Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
- CVE-2023-38159 Windows Graphics Component Elevation of Privilege Vulnerability
- CVE-2023-36902 Windows Runtime Remote Code Execution Vulnerability
- CVE-2023-36776 Win32k Elevation of Privilege Vulnerability
- CVE-2023-36743 Win32k Elevation of Privilege Vulnerability
- CVE-2023-36732 Win32k Elevation of Privilege Vulnerability
- CVE-2023-36731 Win32k Elevation of Privilege Vulnerability
- CVE-2023-36730 Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
- CVE-2023-36729 Named Pipe File System Elevation of Privilege Vulnerability
- CVE-2023-36726 Windows Internet Key Exchange (IKE) Extension Elevation of Privilege Vulnerability
- CVE-2023-36725 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-36724 Windows Power Management Service Information Disclosure Vulnerability
- CVE-2023-36723 Windows Container Manager Service Elevation of Privilege Vulnerability
- CVE-2023-36722 Active Directory Domain Services Information Disclosure Vulnerability
- CVE-2023-36721 Windows Error Reporting Service Elevation of Privilege Vulnerability
- CVE-2023-36720 Windows Mixed Reality Developer Tools Denial of Service Vulnerability
- CVE-2023-36718 Microsoft Virtual Trusted Platform Module Remote Code Execution Vulnerability
- CVE-2023-36717 Windows Virtual Trusted Platform Module Denial of Service

Vulnerability
- CVE-2023-36713 Windows Common Log File System Driver Information Disclosure Vulnerability
- CVE-2023-36712 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-36711 Windows Runtime C++ Template Library Elevation of Privilege Vulnerability
- CVE-2023-36710 Windows Media Foundation Core Remote Code Execution Vulnerability
- CVE-2023-36709 Microsoft AllJoyn API Denial of Service Vulnerability
- CVE-2023-36707 Windows Deployment Services Denial of Service Vulnerability
- CVE-2023-36706 Windows Deployment Services Information Disclosure Vulnerability
- CVE-2023-36704 Windows Setup Files Cleanup Remote Code Execution Vulnerability
- CVE-2023-36703 DHCP Server Service Denial of Service Vulnerability
- CVE-2023-36702 Microsoft DirectMusic Remote Code Execution Vulnerability
- CVE-2023-36701 Microsoft Resilient File System (ReFS) Elevation of Privilege Vulnerability
- CVE-2023-36698 Windows Kernel Security Feature Bypass Vulnerability
- CVE-2023-36697 Microsoft Message Queuing Remote Code Execution Vulnerability
- CVE-2023-36606 Microsoft Message Queuing Denial of Service Vulnerability
- CVE-2023-36605 Windows Named Pipe Filesystem Elevation of Privilege Vulnerability
- CVE-2023-36603 Windows TCP/IP Denial of Service Vulnerability
- CVE-2023-36602 Windows TCP/IP Denial of Service Vulnerability
- CVE-2023-36598 Microsoft WDAC ODBC Driver Remote Code Execution Vulnerability
- CVE-2023-36596 Remote Procedure Call Information Disclosure Vulnerability
- CVE-2023-36594 Windows Graphics Component Elevation of Privilege Vulnerability
- CVE-2023-36593 Microsoft Message Queuing Remote Code Execution Vulnerability
- CVE-2023-36592 Microsoft Message Queuing Remote Code Execution Vulnerability
- CVE-2023-36591 Microsoft Message Queuing Remote Code Execution Vulnerability
- CVE-2023-36590 Microsoft Message Queuing Remote Code Execution Vulnerability
- CVE-2023-36589 Microsoft Message Queuing Remote Code Execution Vulnerability
- CVE-2023-36585 Active Template Library Denial of Service Vulnerability
- CVE-2023-36584 Windows Mark of the Web Security Feature Bypass Vulnerability
- CVE-2023-36583 Microsoft Message Queuing Remote Code Execution Vulnerability
- CVE-2023-36582 Microsoft Message Queuing Remote Code Execution Vulnerability
- CVE-2023-36581 Microsoft Message Queuing Denial of Service Vulnerability
- CVE-2023-36579 Microsoft Message Queuing Denial of Service Vulnerability
- CVE-2023-36578 Microsoft Message Queuing Remote Code Execution Vulnerability
- CVE-2023-36577 Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
- CVE-2023-36576 Windows Kernel Information Disclosure Vulnerability
- CVE-2023-36575 Microsoft Message Queuing Remote Code Execution Vulnerability
- CVE-2023-36574 Microsoft Message Queuing Remote Code Execution Vulnerability
- CVE-2023-36573 Microsoft Message Queuing Remote Code Execution Vulnerability
- CVE-2023-36572 Microsoft Message Queuing Remote Code Execution Vulnerability
- CVE-2023-36571 Microsoft Message Queuing Remote Code Execution Vulnerability
- CVE-2023-36570 Microsoft Message Queuing Remote Code Execution Vulnerability
- CVE-2023-36567 Windows Deployment Services Information Disclosure Vulnerability
- CVE-2023-36564 Windows Search Security Feature Bypass Vulnerability

- CVE-2023-36563 Microsoft WordPad Information Disclosure Vulnerability
- CVE-2023-36557 PrintHTML API Remote Code Execution Vulnerability
- CVE-2023-36438 Windows TCP/IP Information Disclosure Vulnerability
- CVE-2023-36436 Windows MSHTML Platform Remote Code Execution Vulnerability
- CVE-2023-36435 Microsoft QUIC Denial of Service Vulnerability
- CVE-2023-36434 Windows IIS Server Elevation of Privilege Vulnerability
- CVE-2023-36431 Microsoft Message Queuing Denial of Service Vulnerability
- CVE-2023-29349 Microsoft ODBC and OLE DB Remote Code Execution Vulnerability
- CVE-2023-29348 Windows Remote Desktop Gateway (RD Gateway) Information Disclosure 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	KB5031361	windows10.0-kb5031361-x64_961e82abaca6fa50073f65c96143730824956f7d.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5031361	windows10.0-kb5031361-x64_961e82abaca6fa50073f65c96143730824956f7d.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5031362	windows10.0-kb5031362-x86_07d5ba73d10bd140f0b9f5a22a17cf65b35b2c6d.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5031362	windows10.0-kb5031362-x64_d5547372d929a0cfcd12559f75d03507ce6c5d8b.msu	KB4498947 KB4132216
	Windows Server 2016	KB5031362	windows10.0-kb5031362-x64_d5547372d929a0cfcd12559f75d03507ce6c5d8b.msu	KB4498947 KB4132216
BeneVision CMS Viewer	Windows 10 Professional SP1 64bit 1809	KB5031361	windows10.0-kb5031361-x64_961e82abaca6fa50073f65c96143730824956f7d.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5031362	windows10.0-kb5031362-x86_07d5ba73d10bd140f0b9f5a22a17cf65b35b2c6d.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5031362	windows10.0-kb5031362-x64_d5547372d929a0cfcd12559f75d03507ce6c5d8b.msu	KB4498947 KB4132216
Hypervisor X	Windows 10 Professional SP1 64bit 1809	KB5031361	windows10.0-kb5031361-x64_961e82abaca6fa50073f65c96143730824956f7d.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5031361	windows10.0-kb5031361-x64_961e82abaca6fa50073f65c96143730824956f7d.msu	KB5005112 KB5003243

				KB4587735
	Windows 10 1607 for 32-bit	KB5031362	windows10.0-kb5031362-x86_07d5ba73d10bd140f0b9f5a22a17cf65b35b2c6d.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5031362	windows10.0-kb5031362-x64_d5547372d929a0cfcd12559f75d03507ce6c5d8b.msu	KB4498947 KB4132216
eGateway	Windows 10 Professional SP1 64bit 1809	KB5031361	windows10.0-kb5031361-x64_961e82abaca6fa50073f65c96143730824956f7d.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5031361	windows10.0-kb5031361-x64_961e82abaca6fa50073f65c96143730824956f7d.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for x64-based	KB5031362	windows10.0-kb5031362-x64_d5547372d929a0cfcd12559f75d03507ce6c5d8b.msu	KB4498947 KB4132216
	Windows Server 2016	KB5031362	windows10.0-kb5031362-x64_d5547372d929a0cfcd12559f75d03507ce6c5d8b.msu	KB4498947 KB4132216
MLDAP Server	Windows 10 1607 for x64-based	KB5031362	windows10.0-kb5031362-x64_d5547372d929a0cfcd12559f75d03507ce6c5d8b.msu	KB4498947 KB4132216
	Windows Server 2016	KB5031362	windows10.0-kb5031362-x64_d5547372d929a0cfcd12559f75d03507ce6c5d8b.msu	KB4498947 KB4132216
	Windows Server 2019	KB5031361	windows10.0-kb5031361-x64_961e82abaca6fa50073f65c96143730824956f7d.msu	KB5005112 KB5003243 KB4587735
BeneVision Mobile Server	Windows Server 2016	KB5031362	windows10.0-kb5031362-x64_d5547372d929a0cfcd12559f75d03507ce6c5d8b.msu	KB4498947 KB4132216
	Windows Server 2019	KB5031361	windows10.0-kb5031361-x64_961e82abaca6fa50073f65c96143730824956f7d.msu	KB5005112 KB5003243 KB4587735
iView	Windows 10 1607 for x64-based	KB5031362	windows10.0-kb5031362-x64_d5547372d929a0cfcd12559f75d03507ce6c5d8b.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：2023-11-08