

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

**CVE Identifiers**

- CVE-2023-23376 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2023-21823 Windows Graphics Component Remote Code Execution Vulnerability
- CVE-2023-21822 Windows Graphics Component Elevation of Privilege Vulnerability
- CVE-2023-21820 Windows Distributed File System (DFS) Remote Code Execution Vulnerability
- CVE-2023-21819 Windows Secure Channel Denial of Service Vulnerability
- CVE-2023-21818 Windows Secure Channel Denial of Service Vulnerability
- CVE-2023-21817 Windows Kerberos Elevation of Privilege Vulnerability
- CVE-2023-21816 Windows Active Directory Domain Services API Denial of Service Vulnerability
- CVE-2023-21813 Windows Secure Channel Denial of Service Vulnerability
- CVE-2023-21812 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2023-21811 Windows iSCSI Service Denial of Service Vulnerability
- CVE-2023-21805 Windows MSHTML Platform Remote Code Execution Vulnerability
- CVE-2023-21804 Windows Graphics Component Elevation of Privilege Vulnerability
- CVE-2023-21803 Windows iSCSI Discovery Service Remote Code Execution Vulnerability
- CVE-2023-21802 Windows Media Remote Code Execution Vulnerability
- CVE-2023-21801 Microsoft PostScript Printer Driver Remote Code Execution Vulnerability
- CVE-2023-21799 Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
- CVE-2023-21798 Microsoft ODBC Driver Remote Code Execution Vulnerability
- CVE-2023-21797 Microsoft ODBC Driver Remote Code Execution Vulnerability
- CVE-2023-21702 Windows iSCSI Service Denial of Service Vulnerability
- CVE-2023-21701 Microsoft Protected Extensible Authentication Protocol (PEAP) Denial of Service Vulnerability
- CVE-2023-21700 Windows iSCSI Discovery Service Denial of Service Vulnerability
- CVE-2023-21699 Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability
- CVE-2023-21697 Windows Internet Storage Name Service (iSNS) Server Information

Disclosure Vulnerability

- CVE-2023-21695 Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability
- CVE-2023-21694 Windows Fax Service Remote Code Execution Vulnerability
- CVE-2023-21693 Microsoft PostScript Printer Driver Information Disclosure Vulnerability
- CVE-2023-21692 Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability
- CVE-2023-21691 Microsoft Protected Extensible Authentication Protocol (PEAP) Information Disclosure Vulnerability
- CVE-2023-21690 Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability
- CVE-2023-21689 Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability
- CVE-2023-21688 NT OS Kernel Elevation of Privilege Vulnerability
- CVE-2023-21687 HTTP.sys Information Disclosure Vulnerability
- CVE-2023-21686 Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
- CVE-2023-21685 Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
- CVE-2023-21684 Microsoft PostScript Printer Driver Remote Code Execution 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	KB5022840	<a href="#">windows10.0-kb5022840-x64_d7bcae1d048b189823f475e979aba17217cb2892.msu</a>	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5022840	<a href="#">windows10.0-kb5022840-x64_d7bcae1d048b189823f475e979aba17217cb2892.msu</a>	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5022838	<a href="#">windows10.0-kb5022838-x86_6e8241b62e7eb51c4cdcb272963def1a08ac9a5a.msu</a>	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5022838	<a href="#">windows10.0-kb5022838-x64_459501093357a727a15bd3a1101df5e7213b721c.msu</a>	KB4498947 KB4132216
	Windows Server 2012 R2	KB5018922 KB5022894	<a href="#">windows8.1-kb5018922-x64_3aa7832b7586e11304f8fee5e09b6829b32d1833.msu</a> <a href="#">windows8.1-kb5022894-x64_68530c7dd482309a61bbef7ad2a7ea547c649f38.msu</a>	

	Windows Server 2016	KB5022838	<a href="#">windows10.0-kb5022838-x64_459501093357a727a15bd3a1101df5e7213b721c.msu</a>	KB4498947 KB4132216
BeneVision CMS Viewer	Windows 10 Professional SP1 64bit 1809	KB5022840	<a href="#">windows10.0-kb5022840-x64_d7bcae1d048b189823f475e979aba17217cb2892.msu</a>	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5022838	<a href="#">windows10.0-kb5022838-x86_6e8241b62e7eb51c4cdcb272963def1a08ac9a5a.msu</a>	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5022838	<a href="#">windows10.0-kb5022838-x64_459501093357a727a15bd3a1101df5e7213b721c.msu</a>	KB4498947 KB4132216
	Windows Server 2012 R2	KB5018922 KB5022899	<a href="#">windows8.1-kb5018922-x64_3aa7832b7586e11304f8fee5e09b6829b32d1833.msu</a> <a href="#">windows8.1-kb5022899-x64_00d16db3cfdaf18dc89755faebb4aa12aba2cc7.msu</a>	
Hypervisor X CMS	Windows 10 Professional SP1 64bit 1809	KB5022840	<a href="#">windows10.0-kb5022840-x64_d7bcae1d048b189823f475e979aba17217cb2892.msu</a>	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5022840	<a href="#">windows10.0-kb5022840-x64_d7bcae1d048b189823f475e979aba17217cb2892.msu</a>	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5022838	<a href="#">windows10.0-kb5022838-x86_6e8241b62e7eb51c4cdcb272963def1a08ac9a5a.msu</a>	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5022838	<a href="#">windows10.0-kb5022838-x64_459501093357a727a15bd3a1101df5e7213b721c.msu</a>	KB4498947 KB4132216
eGateway	Windows 10 Professional SP1 64bit 1809	KB5022840	<a href="#">windows10.0-kb5022840-x64_d7bcae1d048b189823f475e979aba17217cb2892.msu</a>	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5022840	<a href="#">windows10.0-kb5022840-x64_d7bcae1d048b189823f475e979aba17217cb2892.msu</a>	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for x64-based	KB5022838	<a href="#">windows10.0-kb5022838-x64_459501093357a727a15bd3a1101df5e7213b721c.msu</a>	KB4498947 KB4132216
	Windows Server 2012 R2	KB5018922 KB5022894	<a href="#">windows8.1-kb5018922-x64_3aa7832b7586e11304f8fee5e09b6829b32d1833.msu</a> <a href="#">windows8.1-kb5022894-x64_68530c7dd482309a61bbef7ad2a7ea547c649f38.msu</a>	
	Windows Server 2016	KB5022838	<a href="#">windows10.0-kb5022838-x64_459501093357a727a15bd3a1101df5e7213b721c.msu</a>	KB4498947 KB4132216
MLDAP Server	Windows 10 1607 for x64-based	KB5022840	<a href="#">windows10.0-kb5022840-x64_d7bcae1d048b189823f475e979aba17217cb2892.msu</a>	KB4498947 KB4132216
	Windows Server 2012 R2	KB5018922 KB5022899	<a href="#">windows8.1-kb5018922-x64_3aa7832b7586e11304f8fee5e09b6829b32d1833.msu</a> <a href="#">windows8.1-kb5022899-x64_00d16db3cfdaf18dc89755faebb4aa12aba2cc7.msu</a>	
	Windows Server 2016	KB5022838	<a href="#">windows10.0-kb5022838-x64_459501093357a727a15bd3a1101df5e7213b721c.msu</a>	KB4498947 KB4132216

	Windows Server 2019	KB5022840	<a href="#">windows10.0-kb5022840- x64_d7bcae1d048b189823f475e979aba17217cb2892.msu</a>	KB5005112 KB5003243 KB4587735
BeneVision Mobile Server	Windows Server 2016	KB5022838	<a href="#">windows10.0-kb5022838- x64_459501093357a727a15bd3a1101df5e7213b721c.msu</a>	KB4498947 KB4132216
	Windows Server 2012 R2	KB5018922 KB5022899	<a href="#">windows8.1-kb5018922- x64_3aa7832b7586e11304f8fee5e09b6829b32d1833.msu</a> <a href="#">windows8.1-kb5022899- x64_00d16db3cfdaf18dc89755faebb4aa12aba2cc7.msu</a>	
	Windows Server 2019	KB5022840	<a href="#">windows10.0-kb5022840- x64_d7bcae1d048b189823f475e979aba17217cb2892.msu</a>	KB5005112 KB5003243 KB4587735
iView	Windows 10 1607 for x64-based	KB5022840	<a href="#">windows10.0-kb5022840- x64_d7bcae1d048b189823f475e979aba17217cb2892.msu</a>	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](mailto: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: 2023-3-24