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

CVE Identifiers

- CVE-2023-21776 Windows Kernel Information Disclosure Vulnerability
- CVE-2023-21774 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-21773 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-21772 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-21767 Windows Overlay Filter Elevation of Privilege Vulnerability
- CVE-2023-21766 Windows Overlay Filter Information Disclosure Vulnerability
- CVE-2023-21765 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2023-21760 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2023-21758 Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability
- CVE-2023-21757 Windows Layer 2 Tunneling Protocol (L2TP) Denial of Service Vulnerability
- CVE-2023-21755 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-21754 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-21753 Event Tracing for Windows Information Disclosure Vulnerability
- CVE-2023-21752 Windows Backup Service Elevation of Privilege Vulnerability
- CVE-2023-21750 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-21749 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-21748 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-21747 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-21746 Windows NTLM Elevation of Privilege Vulnerability
- CVE-2023-21739 Windows Bluetooth Driver Elevation of Privilege Vulnerability
- CVE-2023-21732 Microsoft ODBC Driver Remote Code Execution Vulnerability
- CVE-2023-21730 Microsoft Cryptographic Services Elevation of Privilege Vulnerability
- CVE-2023-21728 Windows Netlogon Denial of Service Vulnerability
- CVE-2023-21726 Windows Credential Manager User Interface Elevation of Privilege Vulnerability
- CVE-2023-21683 Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability
- CVE-2023-21682 Windows Point-to-Point Protocol (PPP) Information Disclosure Vulnerability
- CVE-2023-21681 Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
- CVE-2023-21680 Windows Win32k Elevation of Privilege Vulnerability

- CVE-2023-21679 Windows Layer 2 Tunneling Protocol (L2TP) Remote Code Execution Vulnerability
- CVE-2023-21678 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2023-21677 Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability
- CVE-2023-21676 Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
- CVE-2023-21675 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-21674 Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability
- CVE-2023-21563 BitLocker Security Feature Bypass Vulnerability
- CVE-2023-21561 Microsoft Cryptographic Services Elevation of Privilege Vulnerability
- CVE-2023-21560 Windows Boot Manager Security Feature Bypass Vulnerability
- CVE-2023-21559 Windows Cryptographic Information Disclosure Vulnerability
- CVE-2023-21558 Windows Error Reporting Service Elevation of Privilege Vulnerability
- CVE-2023-21557 Windows Lightweight Directory Access Protocol (LDAP) Denial of Service Vulnerability
- CVE-2023-21556 Windows Layer 2 Tunneling Protocol (L2TP) Remote Code Execution Vulnerability
- CVE-2023-21555 Windows Layer 2 Tunneling Protocol (L2TP) Remote Code Execution Vulnerability
- CVE-2023-21552 Windows GDI Elevation of Privilege Vulnerability
- CVE-2023-21551 Microsoft Cryptographic Services Elevation of Privilege Vulnerability
- CVE-2023-21550 Windows Cryptographic Information Disclosure Vulnerability
- CVE-2023-21549 Windows SMB Witness Service Elevation of Privilege Vulnerability
- CVE-2023-21548 Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
- CVE-2023-21547 Internet Key Exchange (IKE) Protocol Denial of Service Vulnerability
- CVE-2023-21546 Windows Layer 2 Tunneling Protocol (L2TP) Remote Code Execution Vulnerability
- CVE-2023-21543 Windows Layer 2 Tunneling Protocol (L2TP) Remote Code Execution Vulnerability
- CVE-2023-21542 Windows Installer Elevation of Privilege Vulnerability
- CVE-2023-21541 Windows Task Scheduler Elevation of Privilege Vulnerability
- CVE-2023-21540 Windows Cryptographic Information Disclosure Vulnerability
- CVE-2023-21537 Microsoft Message Queuing (MSMQ) Elevation of Privilege Vulnerability
- CVE-2023-21536 Event Tracing for Windows Information Disclosure Vulnerability
- CVE-2023-21535 Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
- CVE-2023-21532 Windows GDI Elevation of Privilege Vulnerability
- CVE-2023-21531 Azure Service Fabric Container Elevation of Privilege Vulnerability
- CVE-2023-21527 Windows iSCSI Service Denial of Service Vulnerability
- CVE-2023-21525 Remote Procedure Call Runtime Denial of Service Vulnerability
- CVE-2023-21524 Windows Local Security Authority (LSA) Elevation of Privilege 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	KB5022286	windows10.0-kb5022286-x64_6e84985d215be67ce1395cb2627b5ee68cf4dcb6.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5022286	windows10.0-kb5022286-x64_6e84985d215be67ce1395cb2627b5ee68cf4dcb6.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5022289	windows10.0-kb5022289-x86_4c08c75fd65cbea83479c4e631528582cfc7ee75.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5022289	windows10.0-kb5022289-x64_79d8b59c2bea46d286f2960920c075f416446445.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5022346	windows8.1-kb5022346-x64_ff9f60e266918c364a805db5d49cf763540114ba.msu	
	Windows Server 2016	KB5022289	windows10.0-kb5022289-x64_79d8b59c2bea46d286f2960920c075f416446445.msu	KB4498947 KB4132216
BeneVision CMS Viewer	Windows 10 Professional SP1 64bit 1809	KB5022286	windows10.0-kb5022286-x64_6e84985d215be67ce1395cb2627b5ee68cf4dcb6.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5022289	windows10.0-kb5022289-x86_4c08c75fd65cbea83479c4e631528582cfc7ee75.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5022289	windows10.0-kb5022289-x64_79d8b59c2bea46d286f2960920c075f416446445.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5022352	windows8.1-kb5022352-x64_d625561eda52f6d1f768dc444b817af0650ce81f.msu	
Hypervisor X CMS	Windows 10 Professional SP1 64bit 1809	KB5022286	windows10.0-kb5022286-x64_6e84985d215be67ce1395cb2627b5ee68cf4dcb6.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5022286	windows10.0-kb5022286-x64_6e84985d215be67ce1395cb2627b5ee68cf4dcb6.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5022289	windows10.0-kb5022289-x86_4c08c75fd65cbea83479c4e631528582cfc7ee75.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5022289	windows10.0-kb5022289-x64_79d8b59c2bea46d286f2960920c075f416446445.msu	KB4498947 KB4132216

eGateway	Windows 10 Professional SP1 64bit 1809	KB5022286	windows10.0-kb5022286-x64_6e84985d215be67ce1395cb2627b5ee68cf4dcb6.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5022286	windows10.0-kb5022286-x64_6e84985d215be67ce1395cb2627b5ee68cf4dcb6.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for x64-based	KB5022289	windows10.0-kb5022289-x64_79d8b59c2bea46d286f2960920c075f416446445.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5022346	windows8.1-kb5022346-x64_ff9f60e266918c364a805db5d49cf763540114ba.msu	
	Windows Server 2016	KB5022289	windows10.0-kb5022289-x64_79d8b59c2bea46d286f2960920c075f416446445.msu	KB4498947 KB4132216
MLDAP Server	Windows 10 1607 for x64-based	KB5022289	windows10.0-kb5022289-x64_79d8b59c2bea46d286f2960920c075f416446445.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5022352	windows8.1-kb5022352-x64_d625561eda52f6d1f768dc444b817af0650ce81f.msu	
	Windows Server 2016	KB5022289	windows10.0-kb5022289-x64_79d8b59c2bea46d286f2960920c075f416446445.msu	KB4498947 KB4132216
	Windows Server 2019	KB5022286	windows10.0-kb5022286-x64_6e84985d215be67ce1395cb2627b5ee68cf4dcb6.msu	KB5005112 KB5003243 KB4587735
BeneVision Mobile Server	Windows Server 2016	KB5022289	windows10.0-kb5022289-x64_79d8b59c2bea46d286f2960920c075f416446445.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5022352	windows8.1-kb5022352-x64_d625561eda52f6d1f768dc444b817af0650ce81f.msu	
	Windows Server 2019	KB5022286	windows10.0-kb5022286-x64_6e84985d215be67ce1395cb2627b5ee68cf4dcb6.msu	KB5005112 KB5003243 KB4587735
iView	Windows 10 1607 for x64-based	KB5022289	windows10.0-kb5022289-x64_79d8b59c2bea46d286f2960920c075f416446445.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：2023-02-09