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

CVE Identifiers

- CVE-2023-24913 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
- CVE-2023-24911 Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
- CVE-2023-24910 Windows Graphics Component Elevation of Privilege Vulnerability
- CVE-2023-24909 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
- CVE-2023-24908 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2023-24907 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
- CVE-2023-24906 Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
- CVE-2023-24880 Windows SmartScreen Security Feature Bypass Vulnerability
- CVE-2023-24876 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
- CVE-2023-24872 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
- CVE-2023-24870 Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
- CVE-2023-24869 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2023-24868 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
- CVE-2023-24867 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
- CVE-2023-24866 Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
- CVE-2023-24865 Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
- CVE-2023-24864 Microsoft PostScript and PCL6 Class Printer Driver Elevation of Privilege Vulnerability
- CVE-2023-24863 Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability

- CVE-2023-24862 Windows Secure Channel Denial of Service Vulnerability
- CVE-2023-24861 Windows Graphics Component Elevation of Privilege Vulnerability
- CVE-2023-24859 Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability
- CVE-2023-24858 Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
- CVE-2023-24857 Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
- CVE-2023-24856 Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
- CVE-2023-23423 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-23422 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-23421 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-23420 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-23417 Windows Partition Management Driver Elevation of Privilege Vulnerability
- CVE-2023-23416 Windows Cryptographic Services Remote Code Execution Vulnerability
- CVE-2023-23415 Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability
- CVE-2023-23414 Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability
- CVE-2023-23413 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
- CVE-2023-23412 Windows Accounts Picture Elevation of Privilege Vulnerability
- CVE-2023-23411 Windows Hyper-V Denial of Service Vulnerability
- CVE-2023-23410 Windows HTTP.sys Elevation of Privilege Vulnerability
- CVE-2023-23409 Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability
- CVE-2023-23408 Azure Apache Ambari Spoofing Vulnerability
- CVE-2023-23407 Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability
- CVE-2023-23406 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
- CVE-2023-23405 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2023-23404 Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
- CVE-2023-23403 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
- CVE-2023-23402 Windows Media Remote Code Execution Vulnerability
- CVE-2023-23401 Windows Media Remote Code Execution Vulnerability
- CVE-2023-23400 Windows DNS Server Remote Code Execution Vulnerability
- CVE-2023-23394 Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability
- CVE-2023-23393 Windows Broker Infrastructure Service Elevation of Privilege Vulnerability
- CVE-2023-23388 Windows Bluetooth Driver Elevation of Privilege Vulnerability

- CVE-2023-23385 Windows Point-to-Point Protocol over Ethernet (PPPoE) Elevation of Privilege Vulnerability
- CVE-2023-21708 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2023-1018 CERT/CC: CVE-2023-1018 TPM2.0 Module Library Elevation of Privilege Vulnerability
- CVE-2023-1017 CERT/CC: CVE-2023-1017 TPM2.0 Module Library 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	KB5023702	windows10.0-kb5023702-x64_25c0d04726b1f92c46e76d371ca58875051506c5.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5023702	windows10.0-kb5023702-x64_25c0d04726b1f92c46e76d371ca58875051506c5.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5023697	windows10.0-kb5023697-x86_16d244900507fdd477a2a12dacc89dfd5128c7d6.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5023697	windows10.0-kb5023697-x64_0cde92f5aaba06c1a1bfd64615010c90180dcb86.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5023764	windows8.1-kb5023764-x64_fca6f5dacb913c562e3a66d558caa0b0ff311ab1.msu	
	Windows Server 2016	KB5023697	windows10.0-kb5023697-x64_0cde92f5aaba06c1a1bfd64615010c90180dcb86.msu	KB4498947 KB4132216
BeneVision CMS Viewer	Windows 10 Professional SP1 64bit 1809	KB5023702	windows10.0-kb5023702-x64_25c0d04726b1f92c46e76d371ca58875051506c5.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5023697	windows10.0-kb5023697-x86_16d244900507fdd477a2a12dacc89dfd5128c7d6.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5023697	windows10.0-kb5023697-x64_0cde92f5aaba06c1a1bfd64615010c90180dcb86.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5023765	windows8.1-kb5023765-x64_18c14ac47cdee2cf2329a3f80e176862fe3e4ccb.msu	
Hypervisor X CMS	Windows 10 Professional SP1 64bit 1809	KB5023702	windows10.0-kb5023702-x64_25c0d04726b1f92c46e76d371ca58875051506c5.msu	KB5005112 KB5003243 KB4587735

	Windows Server 2019	KB5023702	windows10.0-kb5023702-x64_25c0d04726b1f92c46e76d371ca58875051506c5.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5023697	windows10.0-kb5023697-x86_16d244900507fdd477a2a12dacc89dfd5128c7d6.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5023697	windows10.0-kb5023697-x64_0cde92f5aaba06c1a1bfd64615010c90180dcb86.msu	KB4498947 KB4132216
eGateway	Windows 10 Professional SP1 64bit 1809	KB5023702	windows10.0-kb5023702-x64_25c0d04726b1f92c46e76d371ca58875051506c5.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5023702	windows10.0-kb5023702-x64_25c0d04726b1f92c46e76d371ca58875051506c5.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for x64-based	KB5023697	windows10.0-kb5023697-x64_0cde92f5aaba06c1a1bfd64615010c90180dcb86.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5023764	windows8.1-kb5023764-x64_fca6f5dacb913c562e3a66d558caa0b0ff311ab1.msu	
	Windows Server 2016	KB5023697	windows10.0-kb5023697-x64_0cde92f5aaba06c1a1bfd64615010c90180dcb86.msu	KB4498947 KB4132216
MLDAP Server	Windows 10 1607 for x64-based	KB5023697	windows10.0-kb5023697-x64_0cde92f5aaba06c1a1bfd64615010c90180dcb86.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5023765	windows8.1-kb5023765-x64_18c14ac47cdee2cf2329a3f80e176862fe3e4ccb.msu	
	Windows Server 2016	KB5023697	windows10.0-kb5023697-x64_0cde92f5aaba06c1a1bfd64615010c90180dcb86.msu	KB4498947 KB4132216
	Windows Server 2019	KB5023702	windows10.0-kb5023702-x64_25c0d04726b1f92c46e76d371ca58875051506c5.msu	KB5005112 KB5003243 KB4587735
BeneVision Mobile Server	Windows Server 2016	KB5023697	windows10.0-kb5023697-x64_0cde92f5aaba06c1a1bfd64615010c90180dcb86.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5023765	windows8.1-kb5023765-x64_18c14ac47cdee2cf2329a3f80e176862fe3e4ccb.msu	
	Windows Server 2019	KB5023702	windows10.0-kb5023702-x64_25c0d04726b1f92c46e76d371ca58875051506c5.msu	KB5005112 KB5003243 KB4587735
iView	Windows 10 1607 for x64-based	KB5023697	windows10.0-kb5023697-x64_0cde92f5aaba06c1a1bfd64615010c90180dcb86.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：2023-4-28