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

CVE Identifiers

- CVE-2023-36719 Microsoft Speech Application Programming Interface (SAPI) Elevation of Privilege Vulnerability
- CVE-2023-36705 Windows Installer Elevation of Privilege Vulnerability
- CVE-2023-36428 Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability
- CVE-2023-36427 Windows Hyper-V Elevation of Privilege Vulnerability
- CVE-2023-36425 Windows Distributed File System (DFS) Remote Code Execution Vulnerability
- CVE-2023-36424 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2023-36423 Microsoft Remote Registry Service Remote Code Execution Vulnerability
- CVE-2023-36408 Windows Hyper-V Elevation of Privilege Vulnerability
- CVE-2023-36405 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-36404 Windows Kernel Information Disclosure Vulnerability
- CVE-2023-36403 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-36402 Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
- CVE-2023-36401 Microsoft Remote Registry Service Remote Code Execution Vulnerability
- CVE-2023-36400 Windows HMAC Key Derivation Elevation of Privilege Vulnerability
- CVE-2023-36398 Windows NTFS Information Disclosure Vulnerability
- CVE-2023-36397 Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability
- CVE-2023-36395 Windows Deployment Services Denial of Service Vulnerability
- CVE-2023-36394 Windows Search Service Elevation of Privilege Vulnerability
- CVE-2023-36393 Windows User Interface Application Core Remote Code Execution Vulnerability
- CVE-2023-36392 DHCP Server Service Denial of Service Vulnerability
- CVE-2023-36047 Windows Authentication Elevation of Privilege Vulnerability
- CVE-2023-36036 Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
- CVE-2023-36033 Windows DWM Core Library Elevation of Privilege Vulnerability
- CVE-2023-36028 Microsoft Protected Extensible Authentication Protocol (PEAP)

Remote Code Execution Vulnerability

- CVE-2023-36025 Windows SmartScreen Security Feature Bypass Vulnerability
- CVE-2023-36017 Windows Scripting Engine Memory Corruption Vulnerability
- CVE-2023-24023 Mitre: CVE-2023-24023 Bluetooth 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	KB5032196	windows10.0-kb5032196-x64_07be38ad94320c193e1e66ee614f2a2c902c1964.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5032196	windows10.0-kb5032196-x64_07be38ad94320c193e1e66ee614f2a2c902c1964.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5032197	windows10.0-kb5032197-x86_c41af0389e0811d11497ed1d094afaa9d66ac6c9.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5032197	windows10.0-kb5032197-x64_7053d3a67b313280f4bf708f519918061c01168d.msu	KB4498947 KB4132216
	Windows Server 2016	KB5032197	windows10.0-kb5032197-x64_7053d3a67b313280f4bf708f519918061c01168d.msu	KB4498947 KB4132216
BeneVision CMS Viewer	Windows 10 Professional SP1 64bit 1809	KB5032196	windows10.0-kb5032196-x64_07be38ad94320c193e1e66ee614f2a2c902c1964.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5032197	windows10.0-kb5032197-x86_c41af0389e0811d11497ed1d094afaa9d66ac6c9.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5032197	windows10.0-kb5032197-x64_7053d3a67b313280f4bf708f519918061c01168d.msu	KB4498947 KB4132216
Hypervisor X	Windows 10 Professional SP1 64bit 1809	KB5032196	windows10.0-kb5032196-x64_07be38ad94320c193e1e66ee614f2a2c902c1964.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5032196	windows10.0-kb5032196-x64_07be38ad94320c193e1e66ee614f2a2c902c1964.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5032197	windows10.0-kb5032197-x86_c41af0389e0811d11497ed1d094afaa9d66ac6c9.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5032197	windows10.0-kb5032197-x64_7053d3a67b313280f4bf708f519918061c01168d.msu	KB4498947 KB4132216

eGateway	Windows 10 Professional SP1 64bit 1809	KB5032196	windows10.0-kb5032196-x64_07be38ad94320c193e1e66ee614f2a2c902c1964.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5032196	windows10.0-kb5032196-x64_07be38ad94320c193e1e66ee614f2a2c902c1964.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for x64-based	KB5032197	windows10.0-kb5032197-x64_7053d3a67b313280f4bf708f519918061c01168d.msu	KB4498947 KB4132216
	Windows Server 2016	KB5032197	windows10.0-kb5032197-x64_7053d3a67b313280f4bf708f519918061c01168d.msu	KB4498947 KB4132216
MLDAP Server	Windows 10 1607 for x64-based	KB5032197	windows10.0-kb5032197-x64_7053d3a67b313280f4bf708f519918061c01168d.msu	KB4498947 KB4132216
	Windows Server 2016	KB5032197	windows10.0-kb5032197-x64_7053d3a67b313280f4bf708f519918061c01168d.msu	KB4498947 KB4132216
	Windows Server 2019	KB5032196	windows10.0-kb5032196-x64_07be38ad94320c193e1e66ee614f2a2c902c1964.msu	KB5005112 KB5003243 KB4587735
BeneVision Mobile Server	Windows Server 2016	KB5032197	windows10.0-kb5032197-x64_7053d3a67b313280f4bf708f519918061c01168d.msu	KB4498947 KB4132216
	Windows Server 2019	KB5032196	windows10.0-kb5032196-x64_07be38ad94320c193e1e66ee614f2a2c902c1964.msu	KB5005112 KB5003243 KB4587735
iView	Windows 10 1607 for x64-based	KB5032197	windows10.0-kb5032197-x64_7053d3a67b313280f4bf708f519918061c01168d.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：2023-12-15