Security Patches for Mindray Products Running on Windows OS (September, 2022)

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 September, 2022. The following CVEs have been evaluated:

CVE Identifiers

- CVE-2022-38006 Windows Graphics Component Information Disclosure Vulnerability
- CVE-2022-38004 Windows Fax Service Remote Code Execution Vulnerability
- CVE-2022-37969 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2022-37959 Network Device Enrollment Service (NDES) Security Feature Bypass Vulnerability
- CVE-2022-37958 SPNEGO Extended Negotiation (NEGOEX) Security Mechanism Information Disclosure Vulnerability
- CVE-2022-37957 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2022-37956 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2022-37955 Windows Group Policy Elevation of Privilege Vulnerability
- CVE-2022-37954 DirectX Graphics Kernel Elevation of Privilege Vulnerability
- CVE-2022-35841 Windows Enterprise App Management Service Remote Code Execution Vulnerability
- CVE-2022-35840 Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
- CVE-2022-35837 Windows Graphics Component Information Disclosure Vulnerability
- CVE-2022-35836 Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
- CVE-2022-35835 Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
- CVE-2022-35834 Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
- CVE-2022-35833 Windows Secure Channel Denial of Service Vulnerability
- CVE-2022-35832 Windows Event Tracing Denial of Service Vulnerability
- CVE-2022-35831 Windows Remote Access Connection Manager Information Disclosure Vulnerability
- CVE-2022-35830 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2022-35803 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2022-34734 Microsoft ODBC Driver Remote Code Execution Vulnerability
- CVE-2022-34733 Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
- CVE-2022-34732 Microsoft ODBC Driver Remote Code Execution Vulnerability

- CVE-2022-34731 Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
- CVE-2022-34730 Microsoft ODBC Driver Remote Code Execution Vulnerability
- CVE-2022-34729 Windows GDI Elevation of Privilege Vulnerability
- CVE-2022-34728 Windows Graphics Component Information Disclosure Vulnerability
- CVE-2022-34727 Microsoft ODBC Driver Remote Code Execution Vulnerability
- CVE-2022-34726 Microsoft ODBC Driver Remote Code Execution Vulnerability
- CVE-2022-34725 Windows ALPC Elevation of Privilege Vulnerability
- CVE-2022-34724 Windows DNS Server Denial of Service Vulnerability
- CVE-2022-34722 Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability
- CVE-2022-34721 Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability
- CVE-2022-34720 Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability
- CVE-2022-34719 Windows Distributed File System (DFS) Elevation of Privilege Vulnerability
- CVE-2022-34718 Windows TCP/IP Remote Code Execution Vulnerability
- CVE-2022-33679 Windows Kerberos Elevation of Privilege Vulnerability
- CVE-2022-33647 Windows Kerberos Elevation of Privilege Vulnerability
- CVE-2022-30200 Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
- CVE-2022-30196 Windows Secure Channel Denial of Service Vulnerability
- CVE-2022-30170 Windows Credential Roaming Service Elevation of Privilege Vulnerability
- CVE-2022-26928 Windows Photo Import API 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	Pre-installed patch
BeneVision CMS	Windows 10 Professional SP1 64bit 1809	KB5017315	windows10.0-kb5017315-x64_611c310985bee4d193a714e702a47b5422918914.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5017315	windows10.0-kb5017315-x64_611c310985bee4d193a714e702a47b5422918914.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5017305	windows10.0-kb5017305-x86_f96f0f3f9c128836bebeb29fa4358077a09dc217.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5017305	windows10.0-kb5016622-x64_77ff4c1d896b008e41f7804648f64ae9bd467f4c.msu	KB4498947 KB4132216

	Windows Server 2012 R2	KB5016683	windows10.0-kb5017305-x64_2c07f36c2861125ecea1098dc29cd03d42c3781b.msu	
	Windows Server 2016	KB5017305	windows10.0-kb5017305-x64_2c07f36c2861125ecea1098dc29cd03d42c3781b.msu	KB4498947 KB4132216
BeneVision CMS Viewer	Windows 10 Professional SP1 64bit 1809	KB5017315	windows10.0-kb5017315-x64_611c310985bee4d193a714e702a47b5422918914.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5017305	windows10.0-kb5017305-x86_f96f0f3f9c128836bebeb29fa4358077a09dc217.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5017305	windows10.0-kb5016622-x64_77ff4c1d896b008e41f7804648f64ae9bd467f4c.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5017367	windows8.1-kb5017367-x64_bb0042f20714b02406713a20e9dc97809d26b538.msu	
Hypervisor X CMS	Windows 10 Professional SP1 64bit 1809	KB5017315	windows10.0-kb5017315-x64_611c310985bee4d193a714e702a47b5422918914.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5017315	windows10.0-kb5017315-x64_611c310985bee4d193a714e702a47b5422918914.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5017305	windows10.0-kb5017305-x86_f96f0f3f9c128836bebeb29fa4358077a09dc217.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5017305	windows10.0-kb5016622-x64_77ff4c1d896b008e41f7804648f64ae9bd467f4c.msu	KB4498947 KB4132216
eGateway	Windows 10 Professional SP1 64bit 1809	KB5017315	windows10.0-kb5017315-x64_611c310985bee4d193a714e702a47b5422918914.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5017315	windows10.0-kb5017315-x64_611c310985bee4d193a714e702a47b5422918914.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for x64-based	KB5017305	windows10.0-kb5017305-x86_f96f0f3f9c128836bebeb29fa4358077a09dc217.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5016683	windows10.0-kb5017305-x64_2c07f36c2861125ecea1098dc29cd03d42c3781b.msu	
	Windows Server 2016	KB5017305	windows10.0-kb5017305-x64_2c07f36c2861125ecea1098dc29cd03d42c3781b.msu	KB4498947 KB4132216
MLDAP Server	Windows 10 1607 for x64-based	KB5017305	windows10.0-kb5017305-x86_f96f0f3f9c128836bebeb29fa435	KB4498947 KB4132216

			8077a09dc217.msu	
	Windows Server 2012 R2	KB5017367	windows8.1-kb5017367-x64_bb0042f20714b02406713a20e9dc97809d26b538.msu	
	Windows Server 2016	KB5017305	windows10.0-kb5017305-x64_2c07f36c2861125ecea1098dc29cd03d42c3781b.msu	KB4498947 KB4132216
	Windows Server 2019	KB5017315	windows10.0-kb5017315-x64_611c310985bee4d193a714e702a47b5422918914.msu	KB5005112 KB5003243 KB4587735
Mobile Server	Windows Server 2016	KB5017305	windows10.0-kb5017305-x64_2c07f36c2861125ecea1098dc29cd03d42c3781b.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5017367	windows8.1-kb5017367-x64_bb0042f20714b02406713a20e9dc97809d26b538.msu	
	Windows Server 2019	KB5017315	windows10.0-kb5017315-x64_611c310985bee4d193a714e702a47b5422918914.msu	KB5005112 KB5003243 KB4587735
iView	Windows 10 1607 for x64-based	KB5016622	windows10.0-kb5017305-x86_f96f0f3f9c128836bebeb29fa4358077a09dc217.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：2022-10-26