Security Patches for Mindray Products Running on Windows OS (December, 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 December, 2022. The following CVEs have been evaluated:

CVE Identifiers

- CVE-2022-44707 Windows Kernel Denial of Service Vulnerability
- CVE-2022-44698 Windows SmartScreen Security Feature Bypass Vulnerability
- CVE-2022-44697 Windows Graphics Component Elevation of Privilege Vulnerability
- CVE-2022-44689 Windows Subsystem for Linux (WSL2) Kernel Elevation of Privilege Vulnerability
- CVE-2022-44683 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2022-44682 Windows Hyper-V Denial of Service Vulnerability
- CVE-2022-44681 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2022-44680 Windows Graphics Component Elevation of Privilege Vulnerability
- CVE-2022-44679 Windows Graphics Component Information Disclosure Vulnerability
- CVE-2022-44678 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2022-44677 Windows Projected File System Elevation of Privilege Vulnerability
- CVE-2022-44676 Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
- CVE-2022-44675 Windows Bluetooth Driver Elevation of Privilege Vulnerability
- CVE-2022-44674 Windows Bluetooth Driver Information Disclosure Vulnerability
- CVE-2022-44673 Windows Client Server Run-Time Subsystem (CSRSS) Elevation of Privilege Vulnerability
- CVE-2022-44671 Windows Graphics Component Elevation of Privilege Vulnerability
- CVE-2022-44670 Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
- CVE-2022-44669 Windows Error Reporting Elevation of Privilege Vulnerability
- CVE-2022-44668 Windows Media Remote Code Execution Vulnerability
- CVE-2022-44667 Windows Media Remote Code Execution Vulnerability
- CVE-2022-44666 Windows Contacts Remote Code Execution Vulnerability
- CVE-2022-41128 Windows Scripting Languages Remote Code Execution Vulnerability
- CVE-2022-41125 Windows CNG Key Isolation Service Elevation of Privilege Vulnerability
- CVE-2022-41121 Windows Graphics Component Elevation of Privilege Vulnerability
- CVE-2022-41118 Windows Scripting Languages Remote Code Execution Vulnerability
- CVE-2022-41113 Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability
- CVE-2022-41109 Windows Win32k Elevation of Privilege Vulnerability
- CVE-2022-41102 Windows Overlay Filter Elevation of Privilege Vulnerability
- CVE-2022-41101 Windows Overlay Filter Elevation of Privilege Vulnerability
- CVE-2022-41100 Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege

Vulnerability
- CVE-2022-41099 BitLocker Security Feature Bypass Vulnerability
- CVE-2022-41098 Windows GDI+ Information Disclosure Vulnerability
- CVE-2022-41097 Network Policy Server (NPS) RADIUS Protocol Information Disclosure Vulnerability
- CVE-2022-41096 Microsoft DWM Core Library Elevation of Privilege Vulnerability
- CVE-2022-41095 Windows Digital Media Receiver Elevation of Privilege Vulnerability
- CVE-2022-41094 Windows Hyper-V Elevation of Privilege Vulnerability
- CVE-2022-41093 Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability
- CVE-2022-41091 Windows Mark of the Web Security Feature Bypass Vulnerability
- CVE-2022-41090 Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability
- CVE-2022-41088 Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
- CVE-2022-41086 Windows Group Policy Elevation of Privilege Vulnerability
- CVE-2022-41077 Windows Fax Compose Form Elevation of Privilege Vulnerability
- CVE-2022-41076 PowerShell Remote Code Execution Vulnerability
- CVE-2022-41074 Windows Graphics Component Information Disclosure Vulnerability
- CVE-2022-41073 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2022-41058 Windows Network Address Translation (NAT) Denial of Service Vulnerability
- CVE-2022-41057 Windows HTTP.sys Elevation of Privilege Vulnerability
- CVE-2022-41056 Network Policy Server (NPS) RADIUS Protocol Denial of Service Vulnerability
- CVE-2022-41055 Windows Human Interface Device Information Disclosure Vulnerability
- CVE-2022-41054 Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability
- CVE-2022-41053 Windows Kerberos Denial of Service Vulnerability
- CVE-2022-41052 Windows Graphics Component Remote Code Execution Vulnerability
- CVE-2022-41050 Windows Extensible File Allocation Table Elevation of Privilege Vulnerability
- CVE-2022-41049 Windows Mark of the Web Security Feature Bypass Vulnerability
- CVE-2022-41048 Microsoft ODBC Driver Remote Code Execution Vulnerability
- CVE-2022-41047 Microsoft ODBC Driver Remote Code Execution Vulnerability
- CVE-2022-41045 Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability
- CVE-2022-41039 Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
- CVE-2022-38023 Netlogon RPC Elevation of Privilege Vulnerability
- CVE-2022-38015 Windows Hyper-V Denial of Service Vulnerability
- CVE-2022-37992 Windows Group Policy Elevation of Privilege Vulnerability
- CVE-2022-37967 Windows Kerberos Elevation of Privilege Vulnerability
- CVE-2022-37966 Windows Kerberos RC4-HMAC Elevation of Privilege Vulnerability
- CVE-2022-23824 AMD: CVE-2022-23824 IBPB and Return Address Predictor Interactions
- ADV220005 Guidance on Microsoft Signed Drivers Being Used Maliciously

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	KB5021237	windows10.0-kb5021237-x64_207fe3b1229757c0a628f2c5c54c8d3068f62d8d.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5021237	windows10.0-kb5021237-x64_207fe3b1229757c0a628f2c5c54c8d3068f62d8d.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5021235	windows10.0-kb5021235-x86_d9f8ad330f3c4a5be2641ba48bc4838e9f3d580f.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5021235	windows10.0-kb5021235-x64_5d51c0893c43763fff710d3c6bc46feb6446d9f1.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5021296	windows8.1-kb5021296-x64_fcc1368eaa82a2ee3d89df254a00d2e25821b121.msu	
	Windows Server 2016	KB5021235	windows10.0-kb5021235-x64_5d51c0893c43763fff710d3c6bc46feb6446d9f1.msu	KB4498947 KB4132216
BeneVision CMS Viewer	Windows 10 Professional SP1 64bit 1809	KB5021237	windows10.0-kb5021237-x64_207fe3b1229757c0a628f2c5c54c8d3068f62d8d.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5021235	windows10.0-kb5021235-x86_d9f8ad330f3c4a5be2641ba48bc4838e9f3d580f.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5021235	windows10.0-kb5021235-x64_5d51c0893c43763fff710d3c6bc46feb6446d9f1.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5021235	windows10.0-kb5021235-x64_5d51c0893c43763fff710d3c6bc46feb6446d9f1.msu	
Hypervisor X CMS	Windows 10 Professional SP1 64bit 1809	KB5021237	windows10.0-kb5021237-x64_207fe3b1229757c0a628f2c5c54c8d3068f62d8d.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5021237	windows10.0-kb5021237-x64_207fe3b1229757c0a628f2c5c54c8d3068f62d8d.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5021235	windows10.0-kb5021235-x86_d9f8ad330f3c4a5be2641ba48bc4838e9f3d580f.msu	KB4498947 KB4132216
	Windows 10 1607	KB5021235	windows10.0-kb5021235-	KB4498947

	for x64-based		x64_5d51c0893c43763fff710d3c6bc46feb6446d9f1.msu	KB4132216
eGateway	Windows 10 Professional SP1 64bit 1809	KB5021237	windows10.0-kb5021237-x64_207fe3b1229757c0a628f2c5c54c8d3068f62d8d.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5021237	windows10.0-kb5021237-x64_207fe3b1229757c0a628f2c5c54c8d3068f62d8d.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for x64-based	KB5021235	windows10.0-kb5021235-x64_5d51c0893c43763fff710d3c6bc46feb6446d9f1.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5021296	windows8.1-kb5021296-x64_fcc1368eaa82a2ee3d89df254a00d2e25821b121.msu	
	Windows Server 2016	KB5021235	windows10.0-kb5021235-x64_5d51c0893c43763fff710d3c6bc46feb6446d9f1.msu	KB4498947 KB4132216
MLDAP Server	Windows 10 1607 for x64-based	KB5021235	windows10.0-kb5021235-x64_5d51c0893c43763fff710d3c6bc46feb6446d9f1.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5021235	windows10.0-kb5021235-x64_5d51c0893c43763fff710d3c6bc46feb6446d9f1.msu	
	Windows Server 2016	KB5021235	windows10.0-kb5021235-x64_5d51c0893c43763fff710d3c6bc46feb6446d9f1.msu	KB4498947 KB4132216
	Windows Server 2019	KB5021237	windows10.0-kb5021237-x64_207fe3b1229757c0a628f2c5c54c8d3068f62d8d.msu	KB5005112 KB5003243 KB4587735
Mobile Server	Windows Server 2016	KB5021235	windows10.0-kb5021235-x64_5d51c0893c43763fff710d3c6bc46feb6446d9f1.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5021235	windows10.0-kb5021235-x64_5d51c0893c43763fff710d3c6bc46feb6446d9f1.msu	
	Windows Server 2019	KB5021237	windows10.0-kb5021237-x64_207fe3b1229757c0a628f2c5c54c8d3068f62d8d.msu	KB5005112 KB5003243 KB4587735
iView	Windows 10 1607 for x64-based	KB5021235	windows10.0-kb5021235-x64_5d51c0893c43763fff710d3c6bc46feb6446d9f1.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：2023-1-18