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

CVE Identifiers

- CVE-2022-35820 Windows Bluetooth Driver Elevation of Privilege Vulnerability
- CVE-2022-35797 Windows Hello Security Feature Bypass Vulnerability
- CVE-2022-35795 Windows Error Reporting Service Elevation of Privilege Vulnerability
- CVE-2022-35794 Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
- CVE-2022-35793 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2022-35792 Storage Spaces Direct Elevation of Privilege Vulnerability
- CVE-2022-35771 Windows Defender Credential Guard Elevation of Privilege Vulnerability
- CVE-2022-35769 Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability
- CVE-2022-35768 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2022-35767 Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
- CVE-2022-35766 Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
- CVE-2022-35765 Storage Spaces Direct Elevation of Privilege Vulnerability
- CVE-2022-35764 Storage Spaces Direct Elevation of Privilege Vulnerability
- CVE-2022-35763 Storage Spaces Direct Elevation of Privilege Vulnerability
- CVE-2022-35762 Storage Spaces Direct Elevation of Privilege Vulnerability
- CVE-2022-35761 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2022-35760 Microsoft ATA Port Driver Elevation of Privilege Vulnerability
- CVE-2022-35759 Windows Local Security Authority (LSA) Denial of Service Vulnerability
- CVE-2022-35758 Windows Kernel Memory Information Disclosure Vulnerability
- CVE-2022-35757 Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
- CVE-2022-35756 Windows Kerberos Elevation of Privilege Vulnerability
- CVE-2022-35755 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2022-35754 Unified Write Filter Elevation of Privilege Vulnerability
- CVE-2022-35753 Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
- CVE-2022-35752 Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
- CVE-2022-35751 Windows Hyper-V Elevation of Privilege Vulnerability
- CVE-2022-35750 Win32k Elevation of Privilege Vulnerability
- CVE-2022-35749 Windows Digital Media Receiver Elevation of Privilege Vulnerability
- CVE-2022-35748 HTTP.sys Denial of Service Vulnerability

- CVE-2022-35747 Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability
- CVE-2022-35746 Windows Digital Media Receiver Elevation of Privilege Vulnerability
- CVE-2022-35745 Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
- CVE-2022-35744 Windows Point-to-Point Protocol (PPP) Remote Code Execution Vulnerability
- CVE-2022-35743 Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability
- CVE-2022-34714 Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
- CVE-2022-34713 Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability
- CVE-2022-34710 Windows Defender Credential Guard Information Disclosure Vulnerability
- CVE-2022-34709 Windows Defender Credential Guard Security Feature Bypass Vulnerability
- CVE-2022-34708 Windows Kernel Information Disclosure Vulnerability
- CVE-2022-34707 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2022-34706 Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability
- CVE-2022-34705 Windows Defender Credential Guard Elevation of Privilege Vulnerability
- CVE-2022-34704 Windows Defender Credential Guard Information Disclosure Vulnerability
- CVE-2022-34703 Windows Partition Management Driver Elevation of Privilege Vulnerability
- CVE-2022-34702 Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability
- CVE-2022-34701 Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability
- CVE-2022-34699 Windows Win32k Elevation of Privilege Vulnerability
- CVE-2022-34696 Windows Hyper-V Remote Code Execution Vulnerability
- CVE-2022-34691 Active Directory Domain Services Elevation of Privilege Vulnerability
- CVE-2022-34690 Windows Fax Service Elevation of Privilege Vulnerability
- CVE-2022-34303 CERT/CC: CVE-20220-34303 Crypto Pro Boot Loader Bypass
- CVE-2022-34302 CERT/CC: CVE-2022-34302 New Horizon Data Systems Inc Boot Loader Bypass
- CVE-2022-34301 CERT/CC: CVE-2022-34301 Eurosoft Boot Loader Bypass
- CVE-2022-33670 Windows Partition Management Driver Elevation of Privilege Vulnerability
- CVE-2022-30197 Windows Kernel Information Disclosure Vulnerability
- CVE-2022-30194 Windows WebBrowser Control Remote Code Execution Vulnerability
- CVE-2022-30144 Windows Bluetooth Service Remote Code Execution Vulnerability
- CVE-2022-30133 Windows Point-to-Point Protocol (PPP) Remote Code Execution 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	KB5016623	windows10.0-kb5016623-x64_c16c09c9b779b8db25b9570a765599f0869b7ee5.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5016623	windows10.0-kb5016623-x64_c16c09c9b779b8db25b9570a765599f0869b7ee5.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5016622	windows10.0-kb5016622-x86_6c37257accbd13d4954e7371375c0a07cbe70955.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5016622	windows10.0-kb5016622-x64_77ff4c1d896b008e41f7804648f64ae9bd467f4c.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5016683	windows8.1-kb5016683-x64_13a8e346779b395cdb33db2acc6548151e54e84c.msu	
	Windows Server 2016	KB5016622	windows10.0-kb5016622-x64_77ff4c1d896b008e41f7804648f64ae9bd467f4c.msu	KB4498947 KB4132216
BeneVision CMS Viewer	Windows 10 Professional SP1 64bit 1809	KB5016623	windows10.0-kb5016623-x64_c16c09c9b779b8db25b9570a765599f0869b7ee5.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5016622	windows10.0-kb5016622-x86_6c37257accbd13d4954e7371375c0a07cbe70955.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5016622	windows10.0-kb5016622-x64_77ff4c1d896b008e41f7804648f64ae9bd467f4c.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5016681	windows8.1-kb5016681-x64_0cd6926c934e163a825b9f18032a5c37f8df7857.msu	
Hypervisor X CMS	Windows 10 Professional SP1 64bit 1809	KB5016623	windows10.0-kb5016623-x64_c16c09c9b779b8db25b9570a765599f0869b7ee5.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5016623	windows10.0-kb5016623-x64_c16c09c9b779b8db25b9570a765599f0869b7ee5.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5016622	windows10.0-kb5016622-x86_6c37257accbd13d4954e7371375c0a07cbe70955.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5016622	windows10.0-kb5016622-x64_77ff4c1d896b008e41f7804648f64ae9bd467f4c.msu	KB4498947 KB4132216
eGateway	Windows 10 Professional SP1	KB5016623	windows10.0-kb5016623-x64_c16c09c9b779b8db25b9570a7	KB5005112 KB5003243

	64bit 1809		65599f0869b7ee5.msu	KB4587735
	Windows Server 2019	KB5016623	windows8.1-kb5016683-x64_13a8e346779b395cdb33db2acc6548151e54e84c.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for x64-based	KB5016622	windows10.0-kb5016622-x86_6c37257accbd13d4954e7371375c0a07cbe70955.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5016683	windows8.1-kb5016683-x64_13a8e346779b395cdb33db2acc6548151e54e84c.msu	
	Windows Server 2016	KB5016622	windows10.0-kb5016622-x64_77ff4c1d896b008e41f7804648f64ae9bd467f4c.msu	KB4498947 KB4132216
MLDAP Server	Windows 10 1607 for x64-based	KB5016622	windows10.0-kb5016622-x86_6c37257accbd13d4954e7371375c0a07cbe70955.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5016681	windows8.1-kb5016681-x64_0cd6926c934e163a825b9f18032a5c37f8df7857.msu	
	Windows Server 2016	KB5016622	windows10.0-kb5016622-x64_77ff4c1d896b008e41f7804648f64ae9bd467f4c.msu	KB4498947 KB4132216
	Windows Server 2019	KB5015811	windows10.0-kb5015811-x64_f850429a022ae53bcebad5e99369adff8b663489.msu	KB5005112 KB5003243 KB4587735
BeneVision Mobile Server	Windows Server 2016	KB5015808	windows10.0-kb5015808-x64_eb7156d8c49c8f23fe3a3f0a3f18b827eeae4530.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5015874	windows8.1-kb5015874-x64_9d92121665dd1f1261bcb941cf6be3144fb92c54.msu	
	Windows Server 2019	KB5016623	windows10.0-kb5016623-x64_c16c09c9b779b8db25b9570a765599f0869b7ee5.msu	KB5005112 KB5003243 KB4587735
iView	Windows 10 1607 for x64-based	KB5016622	windows10.0-kb5016622-x86_6c37257accbd13d4954e7371375c0a07cbe70955.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：2022-9-27