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

CVE Identifiers

- CVE-2022-30226 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2022-30225 Windows Media Player Network Sharing Service Elevation of Privilege Vulnerability
- CVE-2022-30224 Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability
- CVE-2022-30223 Windows Hyper-V Information Disclosure Vulnerability
- CVE-2022-30222 Windows Shell Remote Code Execution Vulnerability
- CVE-2022-30221 Windows Graphics Component Remote Code Execution Vulnerability
- CVE-2022-30220 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2022-30216 Windows Server Service Tampering Vulnerability
- CVE-2022-30215 Active Directory Federation Services Elevation of Privilege Vulnerability
- CVE-2022-30214 Windows DNS Server Remote Code Execution Vulnerability
- CVE-2022-30213 Windows GDI+ Information Disclosure Vulnerability
- CVE-2022-30212 Windows Connected Devices Platform Service Information Disclosure Vulnerability
- CVE-2022-30211 Windows Layer 2 Tunneling Protocol (L2TP) Remote Code Execution Vulnerability
- CVE-2022-30209 Windows IIS Server Elevation of Privilege Vulnerability
- CVE-2022-30208 Windows Security Account Manager (SAM) Denial of Service Vulnerability
- CVE-2022-30206 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2022-30205 Windows Group Policy Elevation of Privilege Vulnerability
- CVE-2022-30203 Windows Boot Manager Security Feature Bypass Vulnerability
- CVE-2022-30202 Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability
- CVE-2022-27776 HackerOne: CVE-2022-27776 Insufficiently protected credentials vulnerability might leak authentication or cookie header data
- CVE-2022-23825 AMD: CVE-2022-23825 AMD CPU Branch Type Confusion
- CVE-2022-23816 AMD: CVE-2022-23816 AMD CPU Branch Type Confusion
- CVE-2022-22711 Windows BitLocker Information Disclosure Vulnerability
- CVE-2022-22050 Windows Fax Service Elevation of Privilege Vulnerability
- CVE-2022-22049 Windows CSRSS Elevation of Privilege Vulnerability
- CVE-2022-22048 BitLocker Security Feature Bypass Vulnerability
- CVE-2022-22047 Windows CSRSS Elevation of Privilege Vulnerability

- CVE-2022-22045 Windows.Devices.Picker.dll Elevation of Privilege Vulnerability
- CVE-2022-22043 Windows Fast FAT File System Driver Elevation of Privilege Vulnerability
- CVE-2022-22042 Windows Hyper-V Information Disclosure Vulnerability
- CVE-2022-22041 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2022-22041 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2022-22040 Internet Information Services Dynamic Compression Module Denial of Service Vulnerability
- CVE-2022-22039 Windows Network File System Remote Code Execution Vulnerability
- CVE-2022-22038 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2022-22037 Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability
- CVE-2022-22036 Performance Counters for Windows Elevation of Privilege Vulnerability
- CVE-2022-22034 Windows Graphics Component Elevation of Privilege Vulnerability
- CVE-2022-22031 Windows Credential Guard Domain-joined Public Key Elevation of Privilege Vulnerability
- CVE-2022-22029 Windows Network File System Remote Code Execution Vulnerability
- CVE-2022-22028 Windows Network File System Information Disclosure Vulnerability
- CVE-2022-22027 Windows Fax Service Remote Code Execution Vulnerability
- CVE-2022-22026 Windows CSRSS Elevation of Privilege Vulnerability
- CVE-2022-22025 Windows Internet Information Services Cachuri Module Denial of Service Vulnerability
- CVE-2022-22024 Windows Fax Service Remote Code Execution Vulnerability
- CVE-2022-22023 Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability
- CVE-2022-22022 Windows Print Spooler 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	KB5015811	windows10.0-kb5015811-x64_f850429a022ae53bcebad5e99369adff8b663489.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5015811	windows10.0-kb5015811-x64_f850429a022ae53bcebad5e99369adff8b663489.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5015808	windows10.0-kb5015808-x86_6af9866887c4f1d096fa7ee6987d307b1c8981f6.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5015808	windows10.0-kb5015808-x64_eb7156d8c49c8f23fe3a3f0a3f18b827eeae4530.msu	KB4498947 KB4132216

	Windows Server 2012 R2	KB5015877	windows8.1-kb5015877-x64_d3398b13ddf93dff3749b53bc0c610207e41ee33.msu	
	Windows Server 2016	KB5015808	windows10.0-kb5015808-x64_eb7156d8c49c8f23fe3a3f0a3f18b827eeae4530.msu	KB4498947 KB4132216
BeneVision CMS Viewer	Windows 10 Professional SP1 64bit 1809	KB5015811	windows10.0-kb5015811-x64_f850429a022ae53bcebad5e99369adff8b663489.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5015808	windows10.0-kb5015808-x64_eb7156d8c49c8f23fe3a3f0a3f18b827eeae4530.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5015808	windows10.0-kb5015808-x86_6af9866887c4f1d096fa7ee6987d307b1c8981f6.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5015874	windows8.1-kb5015874-x64_9d92121665dd1f1261bcb941cf6be3144fb92c54.msu	
Hypervisor X CMS	Windows 10 Professional SP1 64bit 1809	KB5015811	windows10.0-kb5015811-x64_f850429a022ae53bcebad5e99369adff8b663489.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5015811	windows10.0-kb5015811-x64_f850429a022ae53bcebad5e99369adff8b663489.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5015808	windows10.0-kb5015808-x64_eb7156d8c49c8f23fe3a3f0a3f18b827eeae4530.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5015808	windows10.0-kb5015808-x86_6af9866887c4f1d096fa7ee6987d307b1c8981f6.msu	KB4498947 KB4132216
eGateway	Windows 10 Professional SP1 64bit 1809	KB5015811	windows10.0-kb5015811-x64_f850429a022ae53bcebad5e99369adff8b663489.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5015811	windows10.0-kb5015811-x64_f850429a022ae53bcebad5e99369adff8b663489.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for x64-based	KB5015808	windows10.0-kb5015808-x64_eb7156d8c49c8f23fe3a3f0a3f18b827eeae4530.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5015877	windows8.1-kb5015877-x64_d3398b13ddf93dff3749b53bc0c610207e41ee33.msu	
	Windows Server 2016	KB5015808	windows10.0-kb5015808-x64_eb7156d8c49c8f23fe3a3f0a3f18b827eeae4530.msu	KB4498947 KB4132216
MLDAP Server	Windows 10 1607 for x64-based	KB5015808	windows10.0-kb5015808-x64_eb7156d8c49c8f23fe3a3f0a3f1	KB4498947 KB4132216

			8b827eeae4530.msu	
	Windows Server 2012 R2	KB5015874	windows8.1-kb5015874-x64_9d92121665dd1f1261bcb941cf6be3144fb92c54.msu	
	Windows Server 2016	KB5015808	windows10.0-kb5015808-x64_eb7156d8c49c8f23fe3a3f0a3f18b827eeae4530.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	KB5015811	windows10.0-kb5015811-x64_f850429a022ae53bcebad5e99369adff8b663489.msu	KB5005112 KB5003243 KB4587735
iView	Windows 10 1607 for x64-based	KB5015808	windows10.0-kb5015808-x64_eb7156d8c49c8f23fe3a3f0a3f18b827eeae4530.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：2022-8-24