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

CVE Identifiers

- CVE-2022-23256 Azure Data Explorer Spoofing Vulnerability
- CVE-2022-22718 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2022-22717 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2022-22715 Named Pipe File System Elevation of Privilege Vulnerability
- CVE-2022-22712 Windows Hyper-V Denial of Service Vulnerability
- CVE-2022-22710 Windows Common Log File System Driver Denial of Service Vulnerability
- CVE-2022-22002 Windows User Account Profile Picture Denial of Service Vulnerability
- CVE-2022-22001 Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
- CVE-2022-22000 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2022-21999 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2022-21998 Windows Common Log File System Driver Information Disclosure Vulnerability
- CVE-2022-21997 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2022-21996 Win32k Elevation of Privilege Vulnerability
- CVE-2022-21995 Windows Hyper-V Remote Code Execution Vulnerability
- CVE-2022-21994 Windows DWM Core Library Elevation of Privilege Vulnerability
- CVE-2022-21993 Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability
- CVE-2022-21992 Windows Mobile Device Management Remote Code Execution Vulnerability
- CVE-2022-21989 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2022-21986 .NET Denial of Service Vulnerability
- CVE-2022-21985 Windows Remote Access Connection Manager Information Disclosure Vulnerability
- CVE-2022-21985 Windows Remote Access Connection Manager Information Disclosure Vulnerability
- CVE-2022-21984 Windows DNS Server Remote Code Execution Vulnerability
- CVE-2022-21981 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2022-21974 Roaming Security Rights Management Services Remote Code Execution Vulnerability
- CVE-2022-21971 Windows Runtime Remote Code Execution Vulnerability

- CVE-2021-34500 Windows Kernel Memory Information Disclosure Vulnerability
- CVE-2019-0887 Remote Desktop Services Remote Code Execution Vulnerability
- ADV990001 Latest Servicing Stack Updates

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	KB5010351	windows10.0-kb5010351-x64_f7ba53f4c410299fc28400f7a21b7f616f635a7c.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5010351	windows10.0-kb5010351-x64_f7ba53f4c410299fc28400f7a21b7f616f635a7c.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5010359	windows10.0-kb5010359-x86_5c22e4ef70968c563c1880f912ddfa07c7fc4a36.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5010359	windows10.0-kb5010359-x64_f0b427c713754e50609ad0fa7054607a5d404f37.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5010395	windows8.1-kb5010395-x64_0a97e05802268e3f3e0ae07de921f3c1e0c3009b.msu	
	Windows Server 2016	KB5010359	windows10.0-kb5010359-x64_f0b427c713754e50609ad0fa7054607a5d404f37.msu	KB4498947 KB4132216
CMS Viewer	Windows 10 Professional SP1 64bit 1809	KB5010351	windows10.0-kb5010351-x64_f7ba53f4c410299fc28400f7a21b7f616f635a7c.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5010359	windows10.0-kb5010359-x86_5c22e4ef70968c563c1880f912ddfa07c7fc4a36.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5010359	windows10.0-kb5010359-x64_f0b427c713754e50609ad0fa7054607a5d404f37.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5010419	windows8.1-kb5010419-x64_7440cf608ff2a1fe46a71597140c3e32566a4082.msu	
Hypervisor X	Windows 10 Professional SP1 64bit 1809	KB5010351	windows10.0-kb5010351-x64_f7ba53f4c410299fc28400f7a21b7f616f635a7c.msu	KB5005112 KB5003243 KB4587735

	Windows Server 2019	KB5010351	windows10.0-kb5010351-x64_f7ba53f4c410299fc28400f7a21b7f616f635a7c.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit Systems	KB5010359	windows10.0-kb5010359-x86_5c22e4ef70968c563c1880f912ddfa07c7fc4a36.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based Systems	KB5010359	windows10.0-kb5010359-x64_f0b427c713754e50609ad0fa7054607a5d404f37.msu	KB4498947 KB4132216
eGateway	Windows 10 Professional SP1 64bit 1809	KB5010359	windows10.0-kb5010359-x64_f0b427c713754e50609ad0fa7054607a5d404f37.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5010351	windows10.0-kb5010351-x64_f7ba53f4c410299fc28400f7a21b7f616f635a7c.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for x64-based	KB5010351	windows10.0-kb5010359-x64_f0b427c713754e50609ad0fa7054607a5d404f37.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5010395	windows8.1-kb5010395-x64_0a97e05802268e3f3e0ae07de921f3c1e0c3009b.msu	
	Windows Server 2016	KB5010359	windows10.0-kb5010359-x64_f0b427c713754e50609ad0fa7054607a5d404f37.msu	KB4498947 KB4132216
MLDAP Server	Windows 10 1607 for x64-based	KB5010359	windows8.1-kb5010395-x64_0a97e05802268e3f3e0ae07de921f3c1e0c3009b.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5010419	windows8.1-kb5010419-x64_7440cf608ff2a1fe46a71597140c3e32566a4082.msu	
	Windows Server 2016	KB5010359	windows10.0-kb5010359-x64_f0b427c713754e50609ad0fa7054607a5d404f37.msu	KB4498947 KB4132216
	Windows Server 2019	KB5010351	windows10.0-kb5010351-x64_f7ba53f4c410299fc28400f7a21b7f616f635a7c.msu	KB5005112 KB5003243 KB4587735
Mobile Server	Windows Server 2016	KB5010359	windows10.0-kb5010359-x64_f0b427c713754e50609ad0fa7054607a5d404f37.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5010419	windows8.1-kb5010419-x64_7440cf608ff2a1fe46a71597140c3e32566a4082.msu	
	Windows Server 2019	KB5010351	windows10.0-kb5010351-x64_f7ba53f4c410299fc28400f7a21b7f616f635a7c.msu	KB5005112 KB5003243 KB4587735
iView	Windows 10 1607 for x64-based	KB5010359	windows10.0-kb5010359-x64_f0b427c713754e50609ad0fa7	KB4498947 KB4132216

			054607a5d404f37.msu	

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：2022-3-5