Security Patches for Mindray Products Running on Windows OS (April, 2023)

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 April, 2023. The following CVEs have been evaluated:

CVE Identifiers

- CVE-2023-28308 Windows DNS Server Remote Code Execution Vulnerability
- CVE-2023-28307 Windows DNS Server Remote Code Execution Vulnerability
- CVE-2023-28306 Windows DNS Server Remote Code Execution Vulnerability
- CVE-2023-28305 Windows DNS Server Remote Code Execution Vulnerability
- CVE-2023-28302 Microsoft Message Queuing Denial of Service Vulnerability
- CVE-2023-28298 Windows Kernel Denial of Service Vulnerability
- CVE-2023-28297 Windows Remote Procedure Call Service (RPCSS) Elevation of Privilege Vulnerability
- CVE-2023-28293 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-28278 Windows DNS Server Remote Code Execution Vulnerability
- CVE-2023-28276 Windows Group Policy Security Feature Bypass Vulnerability
- CVE-2023-28275 Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability
- CVE-2023-28274 Windows Win32k Elevation of Privilege Vulnerability
- CVE-2023-28273 Windows Clip Service Elevation of Privilege Vulnerability
- CVE-2023-28272 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-28271 Windows Kernel Memory Information Disclosure Vulnerability
- CVE-2023-28270 Windows Lock Screen Security Feature Bypass Vulnerability
- CVE-2023-28269 Windows Boot Manager Security Feature Bypass Vulnerability
- CVE-2023-28268 Netlogon RPC Elevation of Privilege Vulnerability
- CVE-2023-28267 Remote Desktop Protocol Client Information Disclosure Vulnerability
- CVE-2023-28266 Windows Common Log File System Driver Information Disclosure Vulnerability
- CVE-2023-28256 Windows DNS Server Remote Code Execution Vulnerability
- CVE-2023-28255 Windows DNS Server Remote Code Execution Vulnerability
- CVE-2023-28254 Windows DNS Server Remote Code Execution Vulnerability
- CVE-2023-28253 Windows Kernel Information Disclosure Vulnerability
- CVE-2023-28252 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2023-28250 Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability
- CVE-2023-28249 Windows Boot Manager Security Feature Bypass Vulnerability
- CVE-2023-28248 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-28247 Windows Network File System Information Disclosure Vulnerability

- CVE-2023-28244 Windows Kerberos Elevation of Privilege Vulnerability
- CVE-2023-28243 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
- CVE-2023-28241 Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability
- CVE-2023-28240 Windows Network Load Balancing Remote Code Execution Vulnerability
- CVE-2023-28238 Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability
- CVE-2023-28237 Windows Kernel Remote Code Execution Vulnerability
- CVE-2023-28236 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-28235 Windows Lock Screen Security Feature Bypass Vulnerability
- CVE-2023-28232 Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
- CVE-2023-28231 DHCP Server Service Remote Code Execution Vulnerability
- CVE-2023-28229 Windows CNG Key Isolation Service Elevation of Privilege Vulnerability
- CVE-2023-28228 Windows Spoofing Vulnerability
- CVE-2023-28227 Windows Bluetooth Driver Remote Code Execution Vulnerability
- CVE-2023-28226 Windows Enroll Engine Security Feature Bypass Vulnerability
- CVE-2023-28225 Windows NTLM Elevation of Privilege Vulnerability
- CVE-2023-28224 Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability
- CVE-2023-28223 Windows Domain Name Service Remote Code Execution Vulnerability
- CVE-2023-28222 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2023-28221 Windows Error Reporting Service Elevation of Privilege Vulnerability
- CVE-2023-28220 Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
- CVE-2023-28219 Layer 2 Tunneling Protocol Remote Code Execution Vulnerability
- CVE-2023-28218 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
- CVE-2023-28217 Windows Network Address Translation (NAT) Denial of Service Vulnerability
- CVE-2023-28216 Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability
- CVE-2023-24931 Windows Secure Channel Denial of Service Vulnerability
- CVE-2023-24929 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
- CVE-2023-24928 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
- CVE-2023-24927 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
- CVE-2023-24926 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
- CVE-2023-24925 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
- CVE-2023-24924 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability

- CVE-2023-24912 Windows Graphics Component Elevation of Privilege Vulnerability
- CVE-2023-24887 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
- CVE-2023-24886 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
- CVE-2023-24885 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
- CVE-2023-24884 Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability
- CVE-2023-24883 Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability
- CVE-2023-21769 Microsoft Message Queuing Denial of Service Vulnerability
- CVE-2023-21729 Remote Procedure Call Runtime Information Disclosure Vulnerability
- CVE-2023-21727 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2023-21554 Microsoft Message Queuing 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	Necessary Pre-installed patch
BeneVision CMS	Windows 10 Professional SP1 64bit 1809	KB5025229	windows10.0-kb5025229-x64_51315f30dd290d51ba049760d7c107c4b90b27c7.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5025229	windows10.0-kb5023702-x64_25c0d04726b1f92c46e76d371ca58875051506c5.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5025228	windows10.0-kb5025228-x86_0c35a3be0f8cf440a0d0956c3df7eea71ad8b459.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5025228	windows10.0-kb5025228-x64_cd9da61ebd73a46181ba5839bdd59f1fe8e55890.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5025288	windows8.1-kb5025288-x64_93ed37eeee359cce45ee161bcf31d7709887a83a.msu	
	Windows Server 2016	KB5025228	windows10.0-kb5025228-x64_cd9da61ebd73a46181ba5839bdd59f1fe8e55890.msu	KB4498947 KB4132216
BeneVision CMS Viewer	Windows 10 Professional SP1 64bit 1809	KB5025229	windows10.0-kb5025229-x64_51315f30dd290d51ba049760d7c107c4b90b27c7.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5025228	windows10.0-kb5025228-x86_0c35a3be0f8cf440a0d0956c3df7eea71ad8b459.msu	KB4498947 KB4132216

	Windows 10 1607 for x64-based	KB5025228	windows10.0-kb5025228-x64_cd9da61ebd73a46181ba5839bdd59f1fe8e55890.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5025285	windows8.1-kb5025285-x64_f6df5e1bb2e6d0f6a94f12d383e7c1b381406024.msu	
Hypervisor X CMS	Windows 10 Professional SP1 64bit 1809	KB5025229	windows10.0-kb5025229-x64_51315f30dd290d51ba049760d7c107c4b90b27c7.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5025229	windows10.0-kb5023702-x64_25c0d04726b1f92c46e76d371ca58875051506c5.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for 32-bit	KB5025228	windows10.0-kb5025228-x86_0c35a3be0f8cf440a0d0956c3df7eea71ad8b459.msu	KB4498947 KB4132216
	Windows 10 1607 for x64-based	KB5025228	windows10.0-kb5025228-x64_cd9da61ebd73a46181ba5839bdd59f1fe8e55890.msu	KB4498947 KB4132216
eGateway	Windows 10 Professional SP1 64bit 1809	KB5025229	windows10.0-kb5025229-x64_51315f30dd290d51ba049760d7c107c4b90b27c7.msu	KB5005112 KB5003243 KB4587735
	Windows Server 2019	KB5025229	windows10.0-kb5023702-x64_25c0d04726b1f92c46e76d371ca58875051506c5.msu	KB5005112 KB5003243 KB4587735
	Windows 10 1607 for x64-based	KB5025228	windows10.0-kb5025228-x64_cd9da61ebd73a46181ba5839bdd59f1fe8e55890.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5025288	windows8.1-kb5025288-x64_93ed37eeee359cce45ee161bcf31d7709887a83a.msu	
	Windows Server 2016	KB5025228	windows10.0-kb5025228-x64_cd9da61ebd73a46181ba5839bdd59f1fe8e55890.msu	KB4498947 KB4132216
MLDAP Server	Windows 10 1607 for x64-based	KB5025228	windows10.0-kb5025228-x64_cd9da61ebd73a46181ba5839bdd59f1fe8e55890.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5025285	windows8.1-kb5025285-x64_f6df5e1bb2e6d0f6a94f12d383e7c1b381406024.msu	
	Windows Server 2016	KB5025228	windows10.0-kb5025228-x64_cd9da61ebd73a46181ba5839bdd59f1fe8e55890.msu	KB4498947 KB4132216
	Windows Server 2019	KB5025229	windows10.0-kb5023702-x64_25c0d04726b1f92c46e76d371ca58875051506c5.msu	KB5005112 KB5003243 KB4587735
BeneVision Mobile Server	Windows Server 2016	KB5025228	windows10.0-kb5025228-x64_cd9da61ebd73a46181ba5839bdd59f1fe8e55890.msu	KB4498947 KB4132216
	Windows Server 2012 R2	KB5025285	windows8.1-kb5025285-x64_f6df5e1bb2e6d0f6a94f12d383e7c1b381406024.msu	
	Windows Server 2019	KB5025229	windows10.0-kb5023702-x64_25c0d04726b1f92c46e76d371ca58875051506c5.msu	KB5005112 KB5003243 KB4587735

iView	Windows 10 1607 for x64-based	KB5025228	windows10.0-kb5025228-x64_cd9da61ebd73a46181ba5839bdd59f1fe8e55890.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：2023-6-5