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

CVE Identifiers

- CVE-2022-21964 Remote Desktop Licensing Diagnoser Information Disclosure Vulnerability
- CVE-2022-21963 Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
- CVE-2022-21962 Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
- CVE-2022-21961 Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
- CVE-2022-21960 Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
- CVE-2022-21959 Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
- CVE-2022-21958 Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
- CVE-2022-21928 Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
- CVE-2022-21924 Workstation Service Remote Protocol Security Feature Bypass Vulnerability
- CVE-2022-21922 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2022-21921 Windows Defender Credential Guard Security Feature Bypass Vulnerability
- CVE-2022-21920 Windows Kerberos Elevation of Privilege Vulnerability
- CVE-2022-21919 Windows User Profile Service Elevation of Privilege Vulnerability
- CVE-2022-21918 DirectX Graphics Kernel File Denial of Service Vulnerability
- CVE-2022-21916 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2022-21915 Windows GDI+ Information Disclosure Vulnerability
- CVE-2022-21914 Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
- CVE-2022-21913 Local Security Authority (Domain Policy) Remote Protocol Security Feature Bypass
- CVE-2022-21912 DirectX Graphics Kernel Remote Code Execution Vulnerability
- CVE-2022-21910 Microsoft Cluster Port Driver Elevation of Privilege Vulnerability
- CVE-2022-21908 Windows Installer Elevation of Privilege Vulnerability
- CVE-2022-21907 HTTP Protocol Stack Remote Code Execution Vulnerability
- CVE-2022-21906 Windows Defender Application Control Security Feature Bypass Vulnerability
- CVE-2022-21905 Windows Hyper-V Security Feature Bypass Vulnerability
- CVE-2022-21904 Windows GDI Information Disclosure Vulnerability
- CVE-2022-21903 Windows GDI Elevation of Privilege Vulnerability
- CVE-2022-21902 Windows DWM Core Library Elevation of Privilege Vulnerability
- CVE-2022-21901 Windows Hyper-V Elevation of Privilege Vulnerability
- CVE-2022-21900 Windows Hyper-V Security Feature Bypass Vulnerability
- CVE-2022-21899 Windows Extensible Firmware Interface Security Feature Bypass Vulnerability
- CVE-2022-21898 DirectX Graphics Kernel Remote Code Execution Vulnerability
- CVE-2022-21897 Windows Common Log File System Driver Elevation of Privilege Vulnerability

- CVE-2022-21896 Windows DWM Core Library Elevation of Privilege Vulnerability
- CVE-2022-21895 Windows User Profile Service Elevation of Privilege Vulnerability
- CVE-2022-21894 Secure Boot Security Feature Bypass Vulnerability
- CVE-2022-21893 Remote Desktop Protocol Remote Code Execution Vulnerability
- CVE-2022-21892 Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
- CVE-2022-21890 Windows IKE Extension Denial of Service Vulnerability
- CVE-2022-21889 Windows IKE Extension Denial of Service Vulnerability
- CVE-2022-21888 Windows Modern Execution Server Remote Code Execution Vulnerability
- CVE-2022-21887 Win32k Elevation of Privilege Vulnerability
- CVE-2022-21885 Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
- CVE-2022-21884 Local Security Authority Subsystem Service Elevation of Privilege Vulnerability
- CVE-2022-21883 Windows IKE Extension Denial of Service Vulnerability
- CVE-2022-21882 Win32k Elevation of Privilege Vulnerability
- CVE-2022-21881 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2022-21880 Windows GDI+ Information Disclosure Vulnerability
- CVE-2022-21879 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2022-21878 Windows Geolocation Service Remote Code Execution Vulnerability
- CVE-2022-21877 Storage Spaces Controller Information Disclosure Vulnerability
- CVE-2022-21876 Win32k Information Disclosure Vulnerability
- CVE-2022-21875 Windows Storage Elevation of Privilege Vulnerability
- CVE-2022-21874 Windows Security Center API Remote Code Execution Vulnerability
- CVE-2022-21873 Tile Data Repository Elevation of Privilege Vulnerability
- CVE-2022-21872 Windows Event Tracing Elevation of Privilege Vulnerability
- CVE-2022-21871 Microsoft Diagnostics Hub Standard Collector Runtime Elevation of Privilege Vulnerability
- CVE-2022-21870 Tablet Windows User Interface Application Core Elevation of Privilege Vulnerability
- CVE-2022-21869 Clipboard User Service Elevation of Privilege Vulnerability
- CVE-2022-21868 Windows Devices Human Interface Elevation of Privilege Vulnerability
- CVE-2022-21867 Windows Push Notifications Apps Elevation Of Privilege Vulnerability
- CVE-2022-21866 Windows System Launcher Elevation of Privilege Vulnerability
- CVE-2022-21865 Connected Devices Platform Service Elevation of Privilege Vulnerability
- CVE-2022-21864 Windows UI Immersive Server API Elevation of Privilege Vulnerability
- CVE-2022-21863 Windows StateRepository API Server file Elevation of Privilege Vulnerability
- CVE-2022-21862 Windows Application Model Core API Elevation of Privilege Vulnerability
- CVE-2022-21861 Task Flow Data Engine Elevation of Privilege Vulnerability
- CVE-2022-21860 Windows AppContracts API Server Elevation of Privilege Vulnerability
- CVE-2022-21859 Windows Accounts Control Elevation of Privilege Vulnerability
- CVE-2022-21858 Windows Bind Filter Driver Elevation of Privilege Vulnerability
- CVE-2022-21857 Active Directory Domain Services Elevation of Privilege Vulnerability
- CVE-2022-21852 Windows DWM Core Library Elevation of Privilege Vulnerability
- CVE-2022-21851 Remote Desktop Client Remote Code Execution Vulnerability
- CVE-2022-21850 Remote Desktop Client Remote Code Execution Vulnerability
- CVE-2022-21849 Windows IKE Extension Remote Code Execution Vulnerability
- CVE-2022-21848 Windows IKE Extension Denial of Service Vulnerability
- CVE-2022-21847 Windows Hyper-V Denial of Service Vulnerability
- CVE-2022-21843 Windows IKE Extension Denial of Service Vulnerability

- CVE-2022-21839 Windows Event Tracing Discretionary Access Control List Denial of Service Vulnerability
- CVE-2022-21838 Windows Cleanup Manager Elevation of Privilege Vulnerability
- CVE-2022-21837 Microsoft SharePoint Server Remote Code Execution Vulnerability
- CVE-2022-21836 Windows Certificate Spoofing Vulnerability
- CVE-2022-21835 Microsoft Cryptographic Services Elevation of Privilege Vulnerability
- CVE-2022-21834 Windows User-mode Driver Framework Reflector Driver Elevation of Privilege Vulnerability
- CVE-2022-21833 Virtual Machine IDE Drive Elevation of Privilege Vulnerability
- CVE-2021-36976 Libarchive Remote Code Execution Vulnerability
- CVE-2021-22947 Open Source Curl 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:

OS	Hotfix	Product	Download website	Pre-installed patch
Windows 10 Professional SP1 64bit 1809	KB5009557	BeneVision CMS eGateway BeneVision CMS Viewer Hypervisor X CMS	windows10.0-kb5009557-x64_ddc44e498763e16196d8a19dbf4ae54078d31c46.msu	KB5005112 KB5003243 KB4587735
Windows Server 2019	KB5009557	BeneVision CMS eGateway Hypervisor X CMS MLDAP Server BeneVision Mobile Server	windows10.0-kb5009557-x64_ddc44e498763e16196d8a19dbf4ae54078d31c46.msu	KB5005112 KB5003243 KB4587735
Windows 10 Version 1607 for 32-bit Systems	KB5009546	BeneVision CMS Viewer BeneVision CMS Hypervisor X CMS	windows10.0-kb5009546-x86_73496bd12a08c0c89ecddd92473d994a20a763d0.msu	KB4498947 KB4132216
Windows 10 Version 1607 for x64-based Systems Windows Server 2012 R2	KB5009546	BeneVision CMS eGateway BeneVision CMS Viewer MLDAP Server Hypervisor X CMS	windows10.0-kb5009546-x64_d3ab97e9f811d7bf19c268e5e6b5e00e92e110ed.msu	KB4498947 KB4132216
	KB5009595	BeneVision CMS eGateway	windows8.1-kb5009595-x64_9d5677ca5e865931bc908b13139bf266ccbf2922.msu	
Windows Server 2016	KB5009624	BeneVision CMS Viewer BeneVision Mobile Server MLDAP Server	windows8.1-kb5009624-x64_ae9f21e6bcae6274ea54ed380ab0a961aa7d6377.msu	

Windows Server 2016	KB5009546	BeneVision CMS eGateway MLDAP Server BeneVision Mobile Server	windows10.0-kb5009546-x64_d3ab97e9f811d7bf19c268e5e6b5e00e92e110ed.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：2022-2-16