

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 Sep, 2021. The following CVEs have been evaluated:

CVE Identifiers

- CVE-2021-40448 Microsoft Accessibility Insights for Android Information Disclosure Vulnerability
- CVE-2021-40447 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2021-40444 Microsoft MSHTML Remote Code Execution Vulnerability
- CVE-2021-40440 Microsoft Dynamics Business Central Cross-site Scripting Vulnerability
- CVE-2021-38671 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2021-38667 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2021-38661 HEVC Video Extensions Remote Code Execution Vulnerability
- CVE-2021-38660 Microsoft Office Graphics Remote Code Execution Vulnerability
- CVE-2021-38659 Microsoft Office Remote Code Execution Vulnerability
- CVE-2021-38658 Microsoft Office Graphics Remote Code Execution Vulnerability
- CVE-2021-38657 Microsoft Office Graphics Component Information Disclosure Vulnerability
- CVE-2021-38656 Microsoft Word Remote Code Execution Vulnerability
- CVE-2021-38655 Microsoft Excel Remote Code Execution Vulnerability
- CVE-2021-38654 Microsoft Office Visio Remote Code Execution Vulnerability
- CVE-2021-38653 Microsoft Office Visio Remote Code Execution Vulnerability
- CVE-2021-38652 Microsoft SharePoint Server Spoofing Vulnerability
- CVE-2021-38651 Microsoft SharePoint Server Spoofing Vulnerability
- CVE-2021-38650 Microsoft Office Spoofing Vulnerability
- CVE-2021-38649 Open Management Infrastructure Elevation of Privilege Vulnerability
- CVE-2021-38648 Open Management Infrastructure Elevation of Privilege Vulnerability
- CVE-2021-38647 Open Management Infrastructure Remote Code Execution Vulnerability
- CVE-2021-38646 Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability
- CVE-2021-38645 Open Management Infrastructure Elevation of Privilege Vulnerability
- CVE-2021-38644 Microsoft MPEG-2 Video Extension Remote Code Execution Vulnerability
- CVE-2021-38639 Win32k Elevation of Privilege Vulnerability
- CVE-2021-38638 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
- CVE-2021-38637 Windows Storage Information Disclosure Vulnerability
- CVE-2021-38636 Windows Redirected Drive Buffering SubSystem Driver Information

Disclosure Vulnerability

- CVE-2021-38635 Windows Redirected Drive Buffering SubSystem Driver Information Disclosure Vulnerability
- CVE-2021-38634 Microsoft Windows Update Client Elevation of Privilege Vulnerability
- CVE-2021-38633 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2021-38632 BitLocker Security Feature Bypass Vulnerability
- CVE-2021-38630 Windows Event Tracing Elevation of Privilege Vulnerability
- CVE-2021-38629 Windows Ancillary Function Driver for WinSock Information Disclosure Vulnerability
- CVE-2021-38628 Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
- CVE-2021-38626 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2021-38625 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2021-38624 Windows Key Storage Provider Security Feature Bypass Vulnerability
- CVE-2021-36975 Win32k Elevation of Privilege Vulnerability
- CVE-2021-36974 Windows SMB Elevation of Privilege Vulnerability
- CVE-2021-36973 Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability
- CVE-2021-36972 Windows SMB Information Disclosure Vulnerability
- CVE-2021-36969 Windows Redirected Drive Buffering SubSystem Driver Information Disclosure Vulnerability
- CVE-2021-36968 Windows DNS Elevation of Privilege Vulnerability
- CVE-2021-36967 Windows WLAN AutoConfig Service Elevation of Privilege Vulnerability
- CVE-2021-36966 Windows Subsystem for Linux Elevation of Privilege Vulnerability
- CVE-2021-36965 Windows WLAN AutoConfig Service Remote Code Execution Vulnerability
- CVE-2021-36964 Windows Event Tracing Elevation of Privilege Vulnerability
- CVE-2021-36963 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2021-36962 Windows Installer Information Disclosure Vulnerability
- CVE-2021-36961 Windows Installer Denial of Service Vulnerability
- CVE-2021-36960 Windows SMB Information Disclosure Vulnerability
- CVE-2021-36959 Windows Authenticode Spoofing Vulnerability
- CVE-2021-36958 Windows Print Spooler Remote Code Execution Vulnerability
- CVE-2021-36956 Azure Sphere Information Disclosure Vulnerability
- CVE-2021-36955 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2021-36954 Windows Bind Filter Driver Elevation of Privilege Vulnerability
- CVE-2021-36952 Visual Studio Remote Code Execution Vulnerability
- CVE-2021-34442 Windows DNS Server Remote Code Execution Vulnerability
- CVE-2021-30633 Chromium: CVE-2021-30633 Use after free in Indexed DB API
- CVE-2021-30632 Chromium: CVE-2021-30632 Out of bounds write in V8
- CVE-2021-30631 Chromium: CVE-2021-30631 Type Confusion in Blink layout
- CVE-2021-30630 Chromium: CVE-2021-30630 Inappropriate implementation in Blink
- CVE-2021-30629 Chromium: CVE-2021-30629 Use after free in Permissions
- CVE-2021-30628 Chromium: CVE-2021-30628 Stack buffer overflow in ANGLE

- CVE-2021-30627 Chromium: CVE-2021-30627 Type Confusion in Blink layout
- CVE-2021-30626 Chromium: CVE-2021-30626 Out of bounds memory access in ANGLE
- CVE-2021-30625 Chromium: CVE-2021-30625 Use after free in Selection API
- CVE-2021-26437 Visual Studio Code Spoofing Vulnerability
- CVE-2021-26435 Windows Scripting Engine Memory Corruption Vulnerability
- CVE-2021-26434 Visual Studio Elevation of Privilege Vulnerability
- CVE-2021-1678 Windows Print Spooler Spoofing 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:

OS	Hotfix	Product	Download website
Windows 10 Professional SP1 64bit 1809	KB5005568	BeneVision CMS eGateway BeneVision CMS Viewer, Hypervisor X CMS	windows10.0-kb5005568-x64_417d4c6ae0067fcb682dec671d0111a731a0550.msu
Windows 10 Version 1607 for 32-bit Systems	KB5005573	BeneVision CMS Viewer BeneVision CMS Hypervisor X CMS	windows10.0-kb5005573-x86_325f209aa9b767a702ea35e64bd0280185eb956b.msu
Windows 10 Version 1607 for x64-based Systems	KB5005573	BeneVision CMS eGateway BeneVision CMS Viewer, MLDAP Server Hypervisor X CMS	windows10.0-kb5005573-x64_68ae94716592a0f0585b0741ab94840d5b9957de.msu
Windows Server 2012 R2	KB5005627	BeneVision CMS eGateway	windows8.1-kb5005627-x64_830b50ab893c0fe6bda4248311d98555d26fccbd.msu
	KB5005613	BeneVision CMS Viewer, BeneVision Mobile Server, MLDAP Server	windows8.1-kb5005613-x64_52d05012aa71c9d14f218559dba1baa82e4515c9.msu
Windows Server 2016	KB5005573	BeneVision CMS eGateway MLDAP Server BeneVision Mobile Server	windows10.0-kb5005573-x64_68ae94716592a0f0585b0741ab94840d5b9957de.msu
Windows 10 Version 1607 for	KB5005573	iView	windows10.0-kb5005573-x64_68ae94716592a0f0585b0741a

x64-based Systems			b94840d5b9957de.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: 2021-10-24