Security Patches for Mindray Products Running on Windows OS (April, 2021)

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, 2021. The following CVEs have been evaluated:

CVE Identifiers

- CVE-2021-28483 Microsoft Exchange Server Remote Code Execution Vulnerability
- CVE-2021-28482 Microsoft Exchange Server Remote Code Execution Vulnerability
- CVE-2021-28481 Microsoft Exchange Server Remote Code Execution Vulnerability
- CVE-2021-28480 Microsoft Exchange Server Remote Code Execution Vulnerability
- CVE-2021-28477 Visual Studio Code Remote Code Execution Vulnerability
- CVE-2021-28475 Visual Studio Code Remote Code Execution Vulnerability
- CVE-2021-28473 Visual Studio Code Remote Code Execution Vulnerability
- CVE-2021-28472 Visual Studio Code Maven for Java Extension Remote Code Execution Vulnerability
- CVE-2021-28471 Remote Development Extension for Visual Studio Code Remote Code Execution Vulnerability
- CVE-2021-28470 Visual Studio Code GitHub Pull Requests and Issues Extension Remote Code Execution Vulnerability
- CVE-2021-28469 Visual Studio Code Remote Code Execution Vulnerability
- CVE-2021-28468 Raw Image Extension Remote Code Execution Vulnerability
- CVE-2021-28466 Raw Image Extension Remote Code Execution Vulnerability
- CVE-2021-28460 Azure Sphere Unsigned Code Execution Vulnerability
- CVE-2021-28459 Azure DevOps Server Spoofing Vulnerability
- CVE-2021-28458 Azure ms-rest-nodeauth Library Elevation of Privilege Vulnerability
- CVE-2021-28457 Visual Studio Code Remote Code Execution Vulnerability
- CVE-2021-28448 Visual Studio Code Kubernetes Tools Remote Code Execution Vulnerability
- CVE-2021-28447 Windows Early Launch Antimalware Driver Security Feature Bypass Vulnerability
- CVE-2021-28446 Windows Portmapping Information Disclosure Vulnerability
- CVE-2021-28445 Windows Network File System Remote Code Execution Vulnerability
- CVE-2021-28444 Windows Hyper-V Security Feature Bypass Vulnerability
- CVE-2021-28443 Windows Console Driver Denial of Service Vulnerability
- CVE-2021-28442 Windows TCP/IP Information Disclosure Vulnerability
- CVE-2021-28441 Windows Hyper-V Information Disclosure Vulnerability
- CVE-2021-28440 Windows Installer Elevation of Privilege Vulnerability
- CVE-2021-28439 Windows TCP/IP Driver Denial of Service Vulnerability
- CVE-2021-28438 Windows Console Driver Denial of Service Vulnerability
- CVE-2021-28437 Windows Installer Information Disclosure Vulnerability
- CVE-2021-28436 Windows Speech Runtime Elevation of Privilege Vulnerability

- CVE-2021-28435 Windows Event Tracing Information Disclosure Vulnerability
- CVE-2021-28434 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28358 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28357 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28356 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28355 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28354 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28353 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28352 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28351 Windows Speech Runtime Elevation of Privilege Vulnerability
- CVE-2021-28350 Windows GDI+ Remote Code Execution Vulnerability
- CVE-2021-28349 Windows GDI+ Remote Code Execution Vulnerability
- CVE-2021-28348 Windows GDI+ Remote Code Execution Vulnerability
- CVE-2021-28347 Windows Speech Runtime Elevation of Privilege Vulnerability
- CVE-2021-28346 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28345 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28344 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28343 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28342 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28341 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28340 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28339 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28338 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28337 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28336 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28335 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28334 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28333 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28332 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28331 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28330 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28329 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28328 Windows DNS Information Disclosure Vulnerability
- CVE-2021-28328 Windows DNS Information Disclosure Vulnerability
- CVE-2021-28327 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2021-28326 Windows AppX Deployment Server Denial of Service Vulnerability
- CVE-2021-28325 Windows SMB Information Disclosure Vulnerability
- CVE-2021-28325 Windows SMB Information Disclosure Vulnerability
- CVE-2021-28324 Windows SMB Information Disclosure Vulnerability
- CVE-2021-28323 Windows DNS Information Disclosure Vulnerability
- CVE-2021-28322 Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability
- CVE-2021-28321 Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability
- CVE-2021-28320 Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability
- CVE-2021-28319 Windows TCP/IP Driver Denial of Service Vulnerability
- CVE-2021-28318 Windows GDI+ Information Disclosure Vulnerability

- CVE-2021-28317 Microsoft Windows Codecs Library Information Disclosure Vulnerability
- CVE-2021-28316 Windows WLAN AutoConfig Service Security Feature Bypass Vulnerability
- CVE-2021-28315 Windows Media Video Decoder Remote Code Execution Vulnerability
- CVE-2021-28314 Windows Hyper-V Elevation of Privilege Vulnerability
- CVE-2021-28313 Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability
- CVE-2021-28312 Windows NTFS Denial of Service Vulnerability
- CVE-2021-28311 Windows Application Compatibility Cache Denial of Service Vulnerability
- CVE-2021-28310 Win32k Elevation of Privilege Vulnerability
- CVE-2021-28309 Windows Kernel Information Disclosure Vulnerability
- CVE-2021-27096 NTFS Elevation of Privilege Vulnerability
- CVE-2021-27095 Windows Media Video Decoder Remote Code Execution Vulnerability
- CVE-2021-27094 Windows Early Launch Antimalware Driver Security Feature Bypass Vulnerability
- CVE-2021-27093 Windows Kernel Information Disclosure Vulnerability
- CVE-2021-27092 Azure AD Web Sign-in Security Feature Bypass Vulnerability
- CVE-2021-27091 RPC Endpoint Mapper Service Elevation of Privilege Vulnerability
- CVE-2021-27090 Windows Secure Kernel Mode Elevation of Privilege Vulnerability
- CVE-2021-27089 Microsoft Internet Messaging API Remote Code Execution Vulnerability
- CVE-2021-27088 Windows Event Tracing Elevation of Privilege Vulnerability
- CVE-2021-27086 Windows Services and Controller App Elevation of Privilege Vulnerability
- CVE-2021-27079 Windows Media Photo Codec Information Disclosure Vulnerability
- CVE-2021-27072 Win32k Elevation of Privilege Vulnerability
- CVE-2021-27067 Azure DevOps Server and Team Foundation Server Information Disclosure Vulnerability
- CVE-2021-27064 Visual Studio Installer Elevation of Privilege Vulnerability
- CVE-2021-26417 Windows Overlay Filter Information Disclosure Vulnerability
- CVE-2021-26416 Windows Hyper-V Denial of Service Vulnerability
- CVE-2021-26415 Windows Installer Elevation of Privilege Vulnerability
- CVE-2021-26413 Windows Installer Spoofing Vulnerability
- CVE-2021-21221 Chromium: CVE-2021-21221 Insufficient validation of untrusted input in Mojo
- CVE-2021-21220 Chromium: CVE-2021-21220 Insufficient validation of untrusted input in V8 for x86_64
- CVE-2021-21219 Chromium: CVE-2021-21219 Uninitialized Use in PDFium
- CVE-2021-21218 Chromium: CVE-2021-21218 Uninitialized Use in PDFium
- CVE-2021-21217 Chromium: CVE-2021-21217 Uninitialized Use in PDFium
- CVE-2021-21216 Chromium: CVE-2021-21216 Inappropriate implementation in Autofill
- CVE-2021-21215 Chromium: CVE-2021-21215 Inappropriate implementation in Autofill
- CVE-2021-21214 Chromium: CVE-2021-21214 Use after free in Network API
- CVE-2021-21213 Chromium: CVE-2021-21213 Use after free in WebMIDI
- CVE-2021-21212 Chromium: CVE-2021-21212 Incorrect security UI in Network Config UI
- CVE-2021-21211 Chromium: CVE-2021-21211 Inappropriate implementation in Navigation
- CVE-2021-21210 Chromium: CVE-2021-21210 Inappropriate implementation in Network
- CVE-2021-21209 Chromium: CVE-2021-21209 Inappropriate implementation in storage
- CVE-2021-21208 Chromium: CVE-2021-21208 Insufficient data validation in QR scanner
- CVE-2021-21207 Chromium: CVE-2021-21207 Use after free in IndexedDB
- CVE-2021-21206 Chromium: CVE-2021-21206 Use after free in Blink
- CVE-2021-21205 Chromium: CVE-2021-21205 Insufficient policy enforcement in navigation

- CVE-2021-21204 Chromium: CVE-2021-21204 Use after free in Blink
- CVE-2021-21203 Chromium: CVE-2021-21203 Use after free in Blink
- CVE-2021-21202 Chromium: CVE-2021-21202 Use after free in extensions
- CVE-2021-21201 Chromium: CVE-2021-21201 Use after free in permissions
- CVE-2020-17049 Kerberos KDC Security Feature Bypass 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 8.1 for 32-bit systems	KB5001382	BeneVision CMS Viewer	windows8.1-kb5001382-x86_13913c751cb8c3cc19d264cd806d39599e828896.msu
Windows 8.1 for x64-based systems	KB5001382	BeneVision CMS Viewer	windows8.1-kb5001382-x64_b78fb64a69b1bffee0191b9855e27b88bc785dc9.msu
Windows 10 Version 1607 for 32-bit Systems	KB5001347	BeneVision CMS Viewer BeneVision CMS Hypervisor X CMS	windows10.0-kb5001347-x86_da174c95a53d5270f92575c3396b394143e4b68f.msu
Windows 10 Version 1607 for x64-based Systems	KB5001347	BeneVision CMS eGateway BeneVision CMS Viewer, MLDAP Server Hypervisor X CMS	windows10.0-kb5001347-x64_eeba2a1a7376795518efc9a9a46378a5545b52ad.msu
Windows Server 2012 R2	KB5001393	BeneVision CMS eGateway	windows8.1-kb5001393-x64_3da2e11d95d53a08e7011ff163f13c285be43e99.msu
	KB5001382	BeneVision CMS Viewer, BeneVision Mobile Server, MLDAP Server	windows8.1-kb5001382-x64_b78fb64a69b1bffee0191b9855e27b88bc785dc9.msu
Windows Server 2016	KB5001347	BeneVision CMS eGateway MLDAP Server BeneVision Mobile Server	windows10.0-kb5001347-x64_eeba2a1a7376795518efc9a9a46378a5545b52ad.msu
Windows 10 Version 1607 for x64-based Systems	KB5001347	iView	windows10.0-kb5001347-x64_eeba2a1a7376795518efc9a9a46378a5545b52ad.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：2021-5-26