Security Patches for Mindray Products Running on Windows OS (July, 2020)

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 July, 2020. The following CVEs have been evaluated:

CVE Identifiers

- CVE-2020-1351 Microsoft Graphics Component Information Disclosure Vulnerability
- CVE-2020-1354 Windows UPnP Device Host Elevation of Privilege Vulnerability
- CVE-2020-1333 Group Policy Services Policy Processing Elevation of Privilege Vulnerability
- CVE-2020-1361 Windows WalletService Information Disclosure Vulnerability
- CVE-2020-1400 Jet Database Engine Remote Code Execution Vulnerability
- CVE-2020-1468 Windows GDI Information Disclosure Vulnerability
- CVE-2020-1249 Windows Runtime Elevation of Privilege Vulnerability
- CVE-2020-1356 Windows iSCSI Target Service Elevation of Privilege Vulnerability
- CVE-2020-1360 Windows Profile Service Elevation of Privilege Vulnerability
- CVE-2020-1357 Windows System Events Broker Elevation of Privilege Vulnerability
- CVE-2020-1393 Windows Diagnostics Hub Elevation of Privilege Vulnerability
- CVE-2020-1370 Windows Runtime Elevation of Privilege Vulnerability
- CVE-2020-1402 Windows ActiveX Installer Service Elevation of Privilege Vulnerability
- CVE-2020-1389 Windows Kernel Information Disclosure Vulnerability
- CVE-2020-1364 Windows WalletService Denial of Service Vulnerability
- CVE-2020-1362 Windows WalletService Elevation of Privilege Vulnerability
- CVE-2020-1040 Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability
- CVE-2020-1041 Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability
- CVE-2020-1385 Windows Credential Picker Elevation of Privilege Vulnerability
- CVE-2020-1408 Microsoft Graphics Remote Code Execution Vulnerability
- CVE-2020-1344 Windows WalletService Elevation of Privilege Vulnerability
- CVE-2020-1409 DirectWrite Remote Code Execution Vulnerability
- CVE-2020-1352 Windows USO Core Worker Elevation of Privilege Vulnerability
- CVE-2020-1042 Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability
- CVE-2020-1406 Windows Network List Service Elevation of Privilege Vulnerability
- CVE-2020-1410 Windows Address Book Remote Code Execution Vulnerability
- CVE-2020-1085 Windows Function Discovery Service Elevation of Privilege Vulnerability
- CVE-2020-1437 Windows Network Location Awareness Service Elevation of Privilege Vulnerability
- CVE-2020-1358 Windows Resource Policy Information Disclosure Vulnerability
- CVE-2020-1371 Windows Event Logging Service Elevation of Privilege Vulnerability
- CVE-2020-1388 Windows Elevation of Privilege Vulnerability
- ADV200008 Microsoft Guidance for Enabling Request Smuggling Filter on IIS Servers
- CVE-2020-1036 Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability

- CVE-2020-1396 Windows ALPC Elevation of Privilege Vulnerability
- CVE-2020-1398 Windows Lockscreen Elevation of Privilege Vulnerability
- CVE-2020-1421 LNK Remote Code Execution Vulnerability
- CVE-2020-1407 Jet Database Engine Remote Code Execution Vulnerability
- CVE-2020-1267 Local Security Authority Subsystem Service Denial of Service Vulnerability
- CVE-2020-1384 Windows CNG Key Isolation Service Elevation of Privilege Vulnerability
- CVE-2020-1374 Remote Desktop Client Remote Code Execution Vulnerability
- CVE-2020-1434 Windows Sync Host Service Elevation of Privilege Vulnerability
- CVE-2020-1346 Windows Modules Installer Elevation of Privilege Vulnerability
- CVE-2020-1369 Windows WalletService Elevation of Privilege Vulnerability
- CVE-2020-1368 Windows Credential Enrollment Manager Service Elevation of Privilege Vulnerability
- CVE-2020-1427 Windows Network Connections Service Elevation of Privilege Vulnerability
- CVE-2020-1043 Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability
- CVE-2020-1350 Windows DNS Server Remote Code Execution Vulnerability
- CVE-2020-1429 Windows Error Reporting Manager Elevation of Privilege Vulnerability
- CVE-2020-1353 Windows Runtime Elevation of Privilege Vulnerability
- CVE-2020-1435 GDI+ Remote Code Execution Vulnerability
- CVE-2020-1365 Windows Event Logging Service Elevation of Privilege Vulnerability
- CVE-2020-1401 Jet Database Engine Remote Code Execution Vulnerability
- CVE-2020-1411 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2020-1412 Microsoft Graphics Components Remote Code Execution Vulnerability
- CVE-2020-1397 Windows Imaging Component Information Disclosure Vulnerability
- CVE-2020-1390 Windows Network Connections Service Elevation of Privilege Vulnerability
- CVE-2020-1428 Windows Network Connections Service Elevation of Privilege Vulnerability
- CVE-2020-1419 Windows Kernel Information Disclosure Vulnerability
- CVE-2020-1399 Windows Runtime Elevation of Privilege Vulnerability
- CVE-2020-1404 Windows Runtime Elevation of Privilege Vulnerability
- CVE-2020-1420 Windows Error Reporting Information Disclosure Vulnerability
- CVE-2020-1438 Windows Network Connections Service Elevation of Privilege Vulnerability
- CVE-2020-1430 Windows UPnP Device Host Elevation of Privilege Vulnerability
- CVE-2020-1463 Windows SharedStream Library Elevation of Privilege Vulnerability
- CVE-2020-1395 Windows Elevation of Privilege Vulnerability
- CVE-2020-1336 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2020-1413 Windows Runtime Elevation of Privilege 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
Windows 8.1 for 32-bit systems	KB4565541	BeneVision CMS Viewer	windows8.1-kb4565541-x86_a09f127508a83ed516a885a1081bfc5918755e26.msu
Windows 8.1 for	KB4565541	BeneVision CMS Viewer	windows8.1-kb4565541-x64_0df4ae2

x64-based systems			5c382b5337fc592254a266652118ba360.msu
Windows 10 Version 1607 for 32-bit Systems	KB4565511	BeneVision CMS Viewer BeneVision CMS Hypervisor X CMS	windows10.0-kb4565511-x86_54d5ebb90e874e53e9af5222a30b0cd5da6b1be3.msu
Windows 10 Version 1607 for x64-based Systems	KB4565511	BeneVision CMS eGateway BeneVision CMS Viewer MLDAP Server Hypervisor X CMS	windows10.0-kb4565511-x64_5d2481cbc9319147ad3c8f42e07a0ee182909be9.msu
Windows Server 2012 R2	KB4565540	BeneVision CMS eGateway	windows8.1-kb4565540-x64_1eba7b590679d38a1a27e44d93bebc710ebfbc42.msu
	KB4565541	BeneVision CMS Viewer BeneVision Mobile Server MLDAP Server	windows8.1-kb4565541-x64_0df4ae25c382b5337fc592254a266652118ba360.msu
Windows Server 2016	KB4565511	BeneVision CMS eGateway MLDAP Server BeneVision Mobile Server	windows10.0-kb4565511-x64_5d2481cbc9319147ad3c8f42e07a0ee182909be9.msu
Windows 10 Version 1607 for x64-based Systems	KB4565511	iView	windows10.0-kb4565511-x64_5d2481cbc9319147ad3c8f42e07a0ee182909be9.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：2020-08-17