Security Patches for Mindray Products Running on Windows OS (September, 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 September, 2020. The following CVEs have been evaluated:

CVE Identifiers

- CVE-2020-0922 Microsoft COM for Windows Remote Code Execution Vulnerability
- CVE-2020-0951 Windows Defender Application Control Security Feature Bypass Vulnerability
- CVE-2020-1559 Windows Storage Services Elevation of Privilege Vulnerability
- CVE-2020-0648 Windows RSoP Service Application Elevation of Privilege Vulnerability
- CVE-2020-1013 Group Policy Elevation of Privilege Vulnerability
- CVE-2020-0790 Microsoft splwow64 Elevation of Privilege Vulnerability
- CVE-2020-0941 Win32k Information Disclosure Vulnerability
- CVE-2020-0664 Active Directory Information Disclosure Vulnerability
- CVE-2020-1039 Jet Database Engine Remote Code Execution Vulnerability
- CVE-2020-0839 Windows dnsrslvr.dll Elevation of Privilege Vulnerability
- CVE-2020-0718 Active Directory Remote Code Execution Vulnerability
- CVE-2020-1285 GDI+ Remote Code Execution Vulnerability
- CVE-2020-1593 Windows Media Audio Decoder Remote Code Execution Vulnerability
- CVE-2020-1596 TLS Information Disclosure Vulnerability
- CVE-2020-1471 Windows CloudExperienceHost Elevation of Privilege Vulnerability
- CVE-2020-0914 Windows State Repository Service Information Disclosure Vulnerability
- CVE-2020-0837 ADFS Spoofing Vulnerability
- CVE-2020-1491 Windows Function Discovery Service Elevation of Privilege Vulnerability
- CVE-2020-1376 Windows Elevation of Privilege Vulnerability
- CVE-2020-1589 Windows Kernel Information Disclosure Vulnerability
- CVE-2020-1319 Microsoft Windows Codecs Library Remote Code Execution Vulnerability
- CVE-2020-1508 Windows Media Audio Decoder Remote Code Execution Vulnerability
- CVE-2020-0782 Windows Cryptographic Catalog Services Elevation of Privilege Vulnerability
- CVE-2020-1034 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2020-1038 Windows Routing Utilities Denial of Service
- CVE-2020-0911 Windows Modules Installer Elevation of Privilege Vulnerability
- CVE-2020-0838 NTFS Elevation of Privilege Vulnerability
- CVE-2020-1598 Windows UPnP Service Elevation of Privilege Vulnerability
- CVE-2020-0904 Windows Hyper-V Denial of Service Vulnerability
- CVE-2020-0998 Windows Graphics Component Elevation of Privilege Vulnerability
- CVE-2020-0836 Windows DNS Denial of Service Vulnerability
- CVE-2020-1091 Windows Graphics Component Information Disclosure Vulnerability
- CVE-2020-0875 Microsoft splwow64 Information Disclosure Vulnerability
- CVE-2020-1146 Microsoft Store Runtime Elevation of Privilege Vulnerability

- CVE-2020-0761 Active Directory Remote Code Execution Vulnerability
- CVE-2020-1129 Microsoft Windows Codecs Library Remote Code Execution Vulnerability
- CVE-2020-0886 Windows Storage Services Elevation of Privilege Vulnerability
- CVE-2020-0870 Shell infrastructure component Elevation of Privilege Vulnerability
- CVE-2020-1130 Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
- CVE-2020-0908 Windows Text Service Module Remote Code Execution Vulnerability
- CVE-2020-1052 Windows Elevation of Privilege Vulnerability
- CVE-2020-1245 Win32k Elevation of Privilege Vulnerability
- CVE-2020-1031 Windows DHCP Server Information Disclosure Vulnerability
- CVE-2020-1030 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2020-1053 DirectX Elevation of Privilege Vulnerability
- CVE-2020-1033 Windows Kernel Information Disclosure Vulnerability
- CVE-2020-0766 Microsoft Store Runtime Elevation of Privilege Vulnerability
- CVE-2020-0912 Windows Function Discovery SSDP Provider Elevation of Privilege Vulnerability
- CVE-2020-1083 Microsoft Graphics Component Information Disclosure Vulnerability
- CVE-2020-0921 Microsoft Graphics Component Information Disclosure Vulnerability
- CVE-2020-1252 Windows Remote Code Execution Vulnerability
- CVE-2020-1074 Jet Database Engine Remote Code Execution Vulnerability
- CVE-2020-1133 Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
- CVE-2020-0856 Active Directory Information Disclosure Vulnerability
- CVE-2020-1115 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2020-1250 Win32k Information Disclosure Vulnerability
- CVE-2020-1256 Windows GDI Information Disclosure Vulnerability
- CVE-2020-1152 Windows Win32k Elevation of Privilege Vulnerability
- CVE-2020-0997 Windows Camera Codec Pack Remote Code Execution Vulnerability
- CVE-2020-1228 Windows DNS Denial of Service Vulnerability
- CVE-2020-1308 DirectX Elevation of Privilege Vulnerability
- CVE-2020-1097 Windows Graphics Component Information Disclosure Vulnerability
- CVE-2020-16854 Windows Kernel Information Disclosure 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	KB4577066	BeneVision CMS Viewer	windows8.1-kb4577066-x86_efef399537dba5b0086f1fd871ae89964f1ad42c.msu
Windows 8.1 for x64-based systems	KB4577066	BeneVision CMS Viewer	windows8.1-kb4577066-x64_640bbb7de82c25f72f14272d61bd6f9a52a3840f.msu
Windows 10 Version 1607 for 32-bit Systems	KB4577015	BeneVision CMS Viewer BeneVision CMS Hypervisor X CMS	windows10.0-kb4577015-x86_c89b2198d21dd338f88b012fe7558f24248e931f.msu

Windows 10 Version 1607 for x64-based Systems	KB4577015	BeneVision CMS eGateway BeneVision CMS Viewer MLDAP Server Hypervisor X CMS	windows10.0-kb4577015-x64_0e838646b432d7b5360fffd0f12365ca181d475d.msu
Windows Server 2012 R2	KB4577071	BeneVision CMS eGateway	windows8.1-kb4577071-x64_df414a69e87626a18e3070b8b5c9bb2b00070678.msu
	KB4577066	BeneVision CMS Viewer BeneVision Mobile Server MLDAP Server	windows8.1-kb4577066-x64_640bbb7de82c25f72f14272d61bd6f9a52a3840f.msu
Windows Server 2016	KB4577015	BeneVision CMS eGateway MLDAP Server BeneVision Mobile Server	windows10.0-kb4577015-x64_0e838646b432d7b5360fffd0f12365ca181d475d.msu
Windows 10 Version 1607 for x64-based Systems	KB4577015	iView	windows10.0-kb4577015-x64_0e838646b432d7b5360fffd0f12365ca181d475d.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：2020-10-23