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

CVE Identifiers

- CVE-2020-17043 Windows Remote Access Elevation of Privilege Vulnerability
- CVE-2020-17042 Windows Print Spooler Remote Code Execution Vulnerability
- CVE-2020-17041 Windows Print Configuration Elevation of Privilege Vulnerability
- CVE-2020-17040 Windows Hyper-V Security Feature Bypass Vulnerability
- CVE-2020-17040 Windows Hyper-V Security Feature Bypass Vulnerability
- CVE-2020-17037 Windows WalletService Elevation of Privilege Vulnerability
- CVE-2020-17036 Windows Function Discovery SSDP Provider Information Disclosure Vulnerability
- CVE-2020-17036 Windows Function Discovery SSDP Provider Information Disclosure Vulnerability
- CVE-2020-17035 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2020-17034 Windows Remote Access Elevation of Privilege Vulnerability
- CVE-2020-17033 Windows Remote Access Elevation of Privilege Vulnerability
- CVE-2020-17032 Windows Remote Access Elevation of Privilege Vulnerability
- CVE-2020-17031 Windows Remote Access Elevation of Privilege Vulnerability
- CVE-2020-17030 Windows MSCTF Server Information Disclosure Vulnerability
- CVE-2020-17030 Windows MSCTF Server Information Disclosure Vulnerability
- CVE-2020-17028 Windows Remote Access Elevation of Privilege Vulnerability
- CVE-2020-17027 Windows Remote Access Elevation of Privilege Vulnerability
- CVE-2020-17026 Windows Remote Access Elevation of Privilege Vulnerability
- CVE-2020-17025 Windows Remote Access Elevation of Privilege Vulnerability
- CVE-2020-17024 Windows Client Side Rendering Print Provider Elevation of Privilege Vulnerability
- CVE-2020-17014 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2020-17013 Win32k Information Disclosure Vulnerability
- CVE-2020-17013 Win32k Information Disclosure Vulnerability
- CVE-2020-17012 Windows Bind Filter Driver Elevation of Privilege Vulnerability
- CVE-2020-17011 Windows Port Class Library Elevation of Privilege Vulnerability
- CVE-2020-17010 Win32k Elevation of Privilege Vulnerability
- CVE-2020-17007 Windows Error Reporting Elevation of Privilege Vulnerability
- CVE-2020-17001 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2020-17000 Remote Desktop Protocol Client Information Disclosure Vulnerability
- CVE-2020-17000 Remote Desktop Protocol Client Information Disclosure Vulnerability
- CVE-2020-16999 Windows WalletService Information Disclosure Vulnerability

- CVE-2020-16999 Windows WalletService Information Disclosure Vulnerability
- CVE-2020-16997 Remote Desktop Protocol Server Information Disclosure Vulnerability
- CVE-2020-16997 Remote Desktop Protocol Server Information Disclosure Vulnerability
- CVE-2020-1599 Windows Spoofing Vulnerability
- CVE-2020-16892 Windows Image Elevation of Privilege Vulnerability
- CVE-2020-16920 Windows Application Compatibility Client Library Elevation of Privilege Vulnerability
- CVE-2020-16916 Windows COM Server Elevation of Privilege Vulnerability
- CVE-2020-1167 Microsoft Graphics Components Remote Code Execution Vulnerability
- CVE-2020-16973 Windows Backup Service Elevation of Privilege Vulnerability
- CVE-2020-16887 Windows Network Connections Service Elevation of Privilege Vulnerability
- CVE-2020-16900 Windows Event System Elevation of Privilege Vulnerability
- CVE-2020-16889 Windows KernelStream Information Disclosure Vulnerability
- CVE-2020-16935 Windows COM Server Elevation of Privilege Vulnerability
- CVE-2020-16897 NetBT Information Disclosure Vulnerability
- CVE-2020-16896 Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability
- CVE-2020-16902 Windows Installer Elevation of Privilege Vulnerability
- CVE-2020-16894 Windows NAT Denial of Service Vulnerability
- CVE-2020-16891 Windows Hyper-V Remote Code Execution Vulnerability
- CVE-2020-16924 Jet Database Engine Remote Code Execution Vulnerability
- CVE-2020-16911 GDI+ Remote Code Execution Vulnerability
- CVE-2020-16919 Windows Enterprise App Management Service Information Disclosure Vulnerability
- CVE-2020-16922 Windows Spoofing Vulnerability
- CVE-2020-16927 Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability
- CVE-2020-16909 Windows Error Reporting Elevation of Privilege Vulnerability
- CVE-2020-16910 Windows Security Feature Bypass Vulnerability
- CVE-2020-1243 Windows Hyper-V Denial of Service Vulnerability
- CVE-2020-16914 Windows GDI+ Information Disclosure Vulnerability
- CVE-2020-16974 Windows Backup Service Elevation of Privilege Vulnerability
- CVE-2020-16939 Group Policy Elevation of Privilege Vulnerability
- CVE-2020-16923 Microsoft Graphics Components Remote Code Execution Vulnerability
- CVE-2020-16885 Windows Storage VSP Driver Elevation of Privilege Vulnerability
- CVE-2020-16936 Windows Backup Service Elevation of Privilege Vulnerability
- CVE-2020-16912 Windows Backup Service Elevation of Privilege Vulnerability
- CVE-2020-16980 Windows iSCSI Target Service Elevation of Privilege Vulnerability
- CVE-2020-16972 Windows Backup Service Elevation of Privilege Vulnerability
- CVE-2020-16940 Windows - User Profile Service Elevation of Privilege Vulnerability
- CVE-2020-16976 Windows Backup Service Elevation of Privilege Vulnerability
- CVE-2020-16975 Windows Backup Service Elevation of Privilege Vulnerability
- CVE-2020-16967 Windows Camera Codec Pack Remote Code Execution Vulnerability
- CVE-2020-16876 Windows Application Compatibility Client Library Elevation of Privilege Vulnerability
- CVE-2020-0764 Windows Storage Services Elevation of Privilege Vulnerability
- CVE-2020-16968 Windows Camera Codec Pack Remote Code Execution Vulnerability
- CVE-2020-16915 Media Foundation Memory Corruption Vulnerability
- CVE-2020-16905 Windows Error Reporting 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	KB4586845	BeneVision CMS Viewer	windows8.1-kb4586845-x86_d7ba89b850342d7efde447ef5dd9d4c0ed36ff30.msu
Windows 8.1 for x64-based systems	KB4586845	BeneVision CMS Viewer	windows8.1-kb4586845-x64_59301f86b9acdd733fa57dda9c0434f527afd848.msu
Windows 10 Version 1607 for 32-bit Systems	KB4586830	BeneVision CMS Viewer BeneVision CMS Hypervisor X CMS	windows10.0-kb4586830-x86_fa241c063e0dfef578730997c1247c6f0b2dfb49.msu
Windows 10 Version 1607 for x64-based Systems	KB4586830	BeneVision CMS eGateway BeneVision CMS Viewer MLDAP Server Hypervisor X CMS	windows10.0-kb4586830-x64_30c6444c0319caa72579a4c59e2e93d756dc9f21.msu
Windows Server 2012 R2	KB4586823	BeneVision CMS eGateway	windows8.1-kb4586823-x64_2d386223e68585b61154fac5fa1d253807420c98.msu
	KB4586845	BeneVision CMS Viewer BeneVision Mobile Server MLDAP Server	windows8.1-kb4586845-x64_59301f86b9acdd733fa57dda9c0434f527afd848.msu
Windows Server 2016	KB4586830	BeneVision CMS eGateway MLDAP Server BeneVision Mobile Server	windows10.0-kb4586830-x64_30c6444c0319caa72579a4c59e2e93d756dc9f21.msu
Windows 10 Version 1607 for x64-based Systems	KB4586830	iView	windows10.0-kb4586830-x64_30c6444c0319caa72579a4c59e2e93d756dc9f21.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：2020-12-17