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

CVE Identifiers

- CVE-2020-1010 Microsoft Windows Elevation of Privilege Vulnerability
- CVE-2020-1090 Windows Runtime Elevation of Privilege Vulnerability
- CVE-2020-1048 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2020-1124 Windows State Repository Service Elevation of Privilege Vulnerability
- CVE-2020-1028 Media Foundation Memory Corruption Vulnerability
- CVE-2020-1158 Windows Runtime Elevation of Privilege Vulnerability
- CVE-2020-1157 Windows Runtime Elevation of Privilege Vulnerability
- CVE-2020-1112 Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability
- CVE-2020-1125 Windows Runtime Elevation of Privilege Vulnerability
- CVE-2020-1076 Windows Denial of Service Vulnerability
- CVE-2020-1051 Jet Database Engine Remote Code Execution Vulnerability
- CVE-2020-1149 Windows Runtime Elevation of Privilege Vulnerability
- CVE-2020-1021 Windows Error Reporting Elevation of Privilege Vulnerability
- CVE-2020-1077 Windows Runtime Elevation of Privilege Vulnerability
- CVE-2020-1114 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2020-1070 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2020-1071 Windows Remote Access Common Dialog Elevation of Privilege Vulnerability
- CVE-2020-1117 Microsoft Color Management Remote Code Execution Vulnerability
- CVE-2020-1154 Windows Common Log File System Driver Elevation of Privilege Vulnerability
- CVE-2020-1153 Microsoft Graphics Components Remote Code Execution Vulnerability
- CVE-2020-1113 Windows Task Scheduler Security Feature Bypass Vulnerability
- CVE-2020-1179 Windows GDI Information Disclosure Vulnerability
- CVE-2020-1078 Windows Installer Elevation of Privilege Vulnerability
- CVE-2020-1116 Windows CSRSS Information Disclosure Vulnerability
- CVE-2020-1072 Windows Kernel Information Disclosure Vulnerability
- CVE-2020-1126 Media Foundation Memory Corruption Vulnerability
- CVE-2020-1068 Microsoft Windows Elevation of Privilege Vulnerability
- CVE-2020-1132 Windows Error Reporting Manager Elevation of Privilege Vulnerability
- CVE-2020-1079 Microsoft Windows Elevation of Privilege Vulnerability
- CVE-2020-1123 Connected User Experiences and Telemetry Service Denial of Service Vulnerability
- CVE-2020-1067 Windows Remote Code Execution Vulnerability
- CVE-2020-1164 Windows Runtime Elevation of Privilege Vulnerability

- CVE-2020-1176 Jet Database Engine Remote Code Execution Vulnerability
- CVE-2020-1185 Windows State Repository Service Elevation of Privilege Vulnerability
- CVE-2020-1156 Windows Runtime Elevation of Privilege Vulnerability
- CVE-2020-1054 Win32k Elevation of Privilege Vulnerability
- CVE-2020-1143 Win32k Elevation of Privilege Vulnerability
- CVE-2020-1191 Windows State Repository Service Elevation of Privilege Vulnerability
- CVE-2020-1131 Windows State Repository Service Elevation of Privilege Vulnerability
- CVE-2020-1144 Windows State Repository Service Elevation of Privilege Vulnerability
- CVE-2020-1141 Windows GDI Information Disclosure Vulnerability
- CVE-2020-1184 Windows State Repository Service Elevation of Privilege Vulnerability
- CVE-2020-1187 Windows State Repository Service Elevation of Privilege Vulnerability
- CVE-2020-1188 Windows State Repository Service Elevation of Privilege Vulnerability
- CVE-2020-1139 Windows Runtime Elevation of Privilege Vulnerability
- CVE-2020-1186 Windows State Repository Service Elevation of Privilege Vulnerability
- CVE-2020-0963 Windows GDI Information Disclosure Vulnerability
- CVE-2020-1061 Microsoft Script Runtime Remote Code Execution Vulnerability
- CVE-2020-0909 Windows Hyper-V Denial of Service Vulnerability
- CVE-2020-1136 Media Foundation Memory Corruption Vulnerability
- CVE-2020-1084 Connected User Experiences and Telemetry Service Denial of Service Vulnerability
- CVE-2020-1081 Windows Printer Service Elevation of Privilege Vulnerability
- CVE-2020-1175 Jet Database Engine Remote Code Execution Vulnerability
- CVE-2020-1189 Windows State Repository Service Elevation of Privilege Vulnerability
- CVE-2020-1134 Windows State Repository Service Elevation of Privilege Vulnerability
- CVE-2020-1174 Jet Database Engine Remote Code Execution Vulnerability
- CVE-2020-1088 Windows Error Reporting Elevation of Privilege Vulnerability
- CVE-2020-1190 Windows State Repository Service Elevation of Privilege Vulnerability
- CVE-2020-1138 Windows Storage Service Elevation of Privilege Vulnerability
- CVE-2020-1082 Windows Error Reporting Elevation of Privilege Vulnerability
- CVE-2020-1086 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	KB4556846	BeneVision CMS Viewer	windows8.1-kb4556846-x86_f7dbbdaace6800eefdcf607b2a9cd1b98f36c7c2.msu
Windows 8.1 for x64-based systems	KB4556846	BeneVision CMS Viewer	windows8.1-kb4556846-x64_639954ee7a25b5ca99ac6d3fb49fb5fe9a81b7db.msu
Windows 10 Version 1607 for 32-bit Systems	KB4556813	BeneVision CMS Viewer BeneVision CMS Hypervisor X CMS	windows10.0-kb4556813-x86_c00956f0e8f9b1774e69f240069641f099209286.msu

Windows 10 Version 1607 for x64-based Systems	KB4556813	BeneVision CMS eGateway BeneVision CMS Viewer MLDAP Server Hypervisor X CMS	windows10.0-kb4556813-x64_074956aa9f895643ea0768d516375d4a1cd732a2.msu
Windows Server 2012 R2	KB4556853	BeneVision CMS eGateway	windows8.1-kb4556853-x64_85809ff95e80d8d78abac132425b15873a79985f.msu
	KB4556846	BeneVision CMS Viewer BeneVision Mobile Server MLDAP Server	windows8.1-kb4556846-x64_639954ee7a25b5ca99ac6d3fb49fb5fe9a81b7db.msu
Windows Server 2016	KB4556813	BeneVision CMS eGateway MLDAP Server BeneVision Mobile Server	windows10.0-kb4556813-x64_074956aa9f895643ea0768d516375d4a1cd732a2.msu
Windows 10 Version 1607 for x64-based Systems	KB4556813	iView	windows10.0-kb4556813-x64_074956aa9f895643ea0768d516375d4a1cd732a2.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：2020-06-11