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

CVE Identifiers

- CVE-2020-0915 Windows GDI Elevation of Privilege Vulnerability
- CVE-2020-1203 Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability
- CVE-2020-1160 Microsoft Graphics Component Information Disclosure Vulnerability
- CVE-2020-0986 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2020-1264 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2020-1208 Jet Database Engine Remote Code Execution Vulnerability
- CVE-2020-0916 Windows GDI Elevation of Privilege Vulnerability
- CVE-2020-1202 Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability
- CVE-2020-1263 Windows Error Reporting Information Disclosure Vulnerability
- CVE-2020-1247 Win32k Elevation of Privilege Vulnerability
- CVE-2020-1270 Windows WLAN Service Elevation of Privilege Vulnerability
- CVE-2020-1207 Win32k Elevation of Privilege Vulnerability
- CVE-2020-1234 Windows Error Reporting Elevation of Privilege Vulnerability
- CVE-2020-1211 Connected Devices Platform Service Elevation of Privilege Vulnerability
- CVE-2020-1301 Windows SMB Authenticated Remote Code Execution Vulnerability
- CVE-2020-1261 Windows Error Reporting Information Disclosure Vulnerability
- CVE-2020-1241 Windows Kernel Security Feature Bypass Vulnerability
- CVE-2020-1291 Windows Network Connections Service Elevation of Privilege Vulnerability
- CVE-2020-1262 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2020-1266 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2020-1293 Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
- CVE-2020-1334 Windows Runtime Elevation of Privilege Vulnerability
- CVE-2020-1299 LNK Remote Code Execution Vulnerability
- CVE-2020-1235 Windows Runtime Elevation of Privilege Vulnerability
- CVE-2020-1305 Windows State Repository Service Elevation of Privilege Vulnerability
- CVE-2020-1271 Windows Backup Service Elevation of Privilege Vulnerability
- CVE-2020-1281 Windows OLE Remote Code Execution Vulnerability
- CVE-2020-1239 Media Foundation Memory Corruption Vulnerability
- CVE-2020-1246 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2020-1232 Media Foundation Information Disclosure Vulnerability
- CVE-2020-1194 Windows Registry Denial of Service Vulnerability
- CVE-2020-1212 OLE Automation Elevation of Privilege Vulnerability
- CVE-2020-1272 Windows Installer Elevation of Privilege Vulnerability
- CVE-2020-1316 Windows Kernel Elevation of Privilege Vulnerability

- CVE-2020-1196 Windows Print Configuration Elevation of Privilege Vulnerability
- CVE-2020-1283 Windows Denial of Service Vulnerability
- CVE-2020-1278 Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
- CVE-2020-1231 Windows Runtime Elevation of Privilege Vulnerability
- CVE-2020-1251 Win32k Elevation of Privilege Vulnerability
- CVE-2020-1197 Windows Error Reporting Manager Elevation of Privilege Vulnerability
- CVE-2020-1236 Jet Database Engine Remote Code Execution Vulnerability
- CVE-2020-1302 Windows Installer Elevation of Privilege Vulnerability
- CVE-2020-1253 Win32k Elevation of Privilege Vulnerability
- CVE-2020-1257 Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
- CVE-2020-1348 Windows GDI Information Disclosure Vulnerability
- CVE-2020-1300 Windows Remote Code Execution Vulnerability
- CVE-2020-1254 Windows Modules Installer Service Elevation of Privilege Vulnerability
- CVE-2020-1269 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2020-1255 Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability
- CVE-2020-1310 Win32k Elevation of Privilege Vulnerability
- CVE-2020-1311 Component Object Model Elevation of Privilege Vulnerability
- CVE-2020-1279 Windows Lockscreen Elevation of Privilege Vulnerability
- CVE-2020-1304 Windows Runtime Elevation of Privilege Vulnerability
- CVE-2020-1317 Group Policy Elevation of Privilege Vulnerability
- CVE-2020-1282 Windows Runtime Elevation of Privilege Vulnerability
- CVE-2020-1287 Windows WalletService Elevation of Privilege Vulnerability
- CVE-2020-1314 Windows Text Service Framework Elevation of Privilege Vulnerability
- CVE-2020-1309 Microsoft Store Runtime Elevation of Privilege Vulnerability
- CVE-2020-1294 Windows WalletService Elevation of Privilege Vulnerability
- CVE-2020-1259 Windows Host Guardian Service Security Feature Bypass 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	KB4561666	BeneVision CMS Viewer	windows8.1-kb4561666-x86_915ba0d35b2682c619ce826de416cbfe8cb5732e.msu
Windows 8.1 for x64-based systems	KB4561666	BeneVision CMS Viewer	windows8.1-kb4561666-x64_9425ca5e1d2f3731ed0263b2b22c3a6981eed91b.msu
Windows 10 Version 1607 for 32-bit Systems	KB4561616	BeneVision CMS Viewer BeneVision CMS Hypervisor X CMS	windows10.0-kb4561616-x86_0abc7112cfebd0cf18468f6c2ce477b332bf5b7e.msu
Windows 10 Version 1607 for x64-based Systems	KB4561616	BeneVision CMS eGateway BeneVision CMS Viewer	windows10.0-kb4561616-x64_0026760a6c77d1a8113855bd853f3c2ea22ada84.msu

		MLDAP Server Hypervisor X CMS	
Windows Server 2012 R2	KB4561673	BeneVision CMS eGateway	windows8.1-kb4561673-x64_d33f29fc2c191f27f6e3181767f06313ddfe33d8.msu
	KB4561666	BeneVision CMS Viewer BeneVision Mobile Server MLDAP Server	windows8.1-kb4561666-x64_9425ca5e1d2f3731ed0263b2b22c3a6981eed91b.msu
Windows Server 2016	KB4561616	BeneVision CMS eGateway MLDAP Server BeneVision Mobile Server	windows10.0-kb4561616-x64_0026760a6c77d1a8113855bd853f3c2ea22ada84.msu
Windows 10 Version 1607 for x64-based Systems	KB4561616	iView	windows10.0-kb4561616-x64_0026760a6c77d1a8113855bd853f3c2ea22ada84.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：2020-07-09