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

CVE Identifiers

- CVE-2020-17140 Windows SMB Information Disclosure Vulnerability
- CVE-2020-17139 Windows Overlay Filter Security Feature Bypass Vulnerability
- CVE-2020-17138 Windows Error Reporting Information Disclosure Vulnerability
- CVE-2020-17138 Windows Error Reporting Information Disclosure Vulnerability
- CVE-2020-17136 Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
- CVE-2020-17134 Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
- CVE-2020-17103 Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
- CVE-2020-17099 Windows Lock Screen Security Feature Bypass Vulnerability
- CVE-2020-17099 Windows Lock Screen Security Feature Bypass Vulnerability
- CVE-2020-17097 Windows Digital Media Receiver Elevation of Privilege Vulnerability
- CVE-2020-17096 Windows NTFS Remote Code Execution Vulnerability
- CVE-2020-17096 Windows NTFS Remote Code Execution Vulnerability
- CVE-2020-17095 Hyper-V Remote Code Execution Vulnerability
- CVE-2020-17095 Hyper-V Remote Code Execution Vulnerability
- CVE-2020-17094 Windows Error Reporting Information Disclosure Vulnerability
- CVE-2020-17094 Windows Error Reporting Information Disclosure Vulnerability
- CVE-2020-17092 Windows Network Connections Service Elevation of Privilege Vulnerability
- CVE-2020-16996 Kerberos Security Feature Bypass Vulnerability
- CVE-2020-16996 Kerberos Security Feature Bypass Vulnerability
- CVE-2020-16964 Windows Backup Engine Elevation of Privilege Vulnerability
- CVE-2020-16963 Windows Backup Engine Elevation of Privilege Vulnerability
- CVE-2020-16962 Windows Backup Engine Elevation of Privilege Vulnerability
- CVE-2020-16961 Windows Backup Engine Elevation of Privilege Vulnerability
- CVE-2020-16960 Windows Backup Engine Elevation of Privilege Vulnerability
- CVE-2020-16959 Windows Backup Engine Elevation of Privilege Vulnerability
- CVE-2020-16958 Windows Backup Engine Elevation of Privilege Vulnerability
- ADV200013 Microsoft Guidance for Addressing Spoofing Vulnerability in DNS Resolver

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	KB4592484	BeneVision CMS Viewer	windows8.1-kb4592484-x86_2a058f1098386f85d106c11dc8f646adf1c6dc3f.msu
Windows 8.1 for x64-based systems	KB4592484	BeneVision CMS Viewer	windows8.1-kb4592484-x64_de40107ba0282603bbeb96f655bb06334ee41e6a.msu
Windows 10 Version 1607 for 32-bit Systems	KB4593226	BeneVision CMS Viewer BeneVision CMS Hypervisor X CMS	windows10.0-kb4593226-x86_d3453294f1a6a23b74e0713593862cd0ccec92df.msu
Windows 10 Version 1607 for x64-based Systems	KB4593226	BeneVision CMS eGateway BeneVision CMS Viewer, MLDAP Server Hypervisor X CMS	windows10.0-kb4593226-x64_d58938ce2e7c111c8e8f0c0bdc80f0e57defbf4d.msu
Windows Server 2012 R2	KB4592495	BeneVision CMS eGateway	windows8.1-kb4592495-x64_3e1dde02bebbe5e66e218da08be0e90f9a077e76.msu
	KB4592484	BeneVision CMS Viewer, BeneVision Mobile Server, MLDAP Server	windows8.1-kb4592484-x64_de40107ba0282603bbeb96f655bb06334ee41e6a.msu
Windows Server 2016	KB4593226	BeneVision CMS eGateway MLDAP Server BeneVision Mobile Server	windows10.0-kb4593226-x64_d58938ce2e7c111c8e8f0c0bdc80f0e57defbf4d.msu
Windows 10 Version 1607 for x64-based Systems	KB4593226	iView	windows10.0-kb4593226-x64_d58938ce2e7c111c8e8f0c0bdc80f0e57defbf4d.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：2021-1-23