Security Patches for Mindray Products Running on Windows OS (May, 2022)

**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, 2022. The following CVEs have been evaluated:

## CVE Identifiers

- CVE-2022-30130 .NET Framework Denial of Service Vulnerability
- CVE-2022-30129 Visual Studio Code Remote Code Execution Vulnerability
- CVE-2022-29972 Insight Software: CVE-2022-29972 Magnitude Simba Amazon Redshift ODBC Driver
- CVE-2022-29151 Windows Cluster Shared Volume (CSV) Elevation of Privilege Vulnerability
- CVE-2022-29150 Windows Cluster Shared Volume (CSV) Elevation of Privilege Vulnerability
- CVE-2022-29142 Windows Kernel Elevation of Privilege Vulnerability
- CVE-2022-29141 Windows LDAP Remote Code Execution Vulnerability
- CVE-2022-29140 Windows Print Spooler Information Disclosure Vulnerability
- CVE-2022-29139 Windows LDAP Remote Code Execution Vulnerability
- CVE-2022-29138 Windows Clustered Shared Volume Elevation of Privilege Vulnerability
- CVE-2022-29137 Windows LDAP Remote Code Execution Vulnerability
- CVE-2022-29135 Windows Cluster Shared Volume (CSV) Elevation of Privilege Vulnerability
- CVE-2022-29134 Windows Clustered Shared Volume Information Disclosure Vulnerability
- CVE-2022-29132 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2022-29131 Windows LDAP Remote Code Execution Vulnerability
- CVE-2022-29130 Windows LDAP Remote Code Execution Vulnerability
- CVE-2022-29129 Windows LDAP Remote Code Execution Vulnerability
- CVE-2022-29128 Windows LDAP Remote Code Execution Vulnerability
- CVE-2022-29127 BitLocker Security Feature Bypass Vulnerability
- CVE-2022-29126 Tablet Windows User Interface Application Core Elevation of Privilege Vulnerability
- CVE-2022-29125 Windows Push Notifications Apps Elevation of Privilege Vulnerability
- CVE-2022-29123 Windows Clustered Shared Volume Information Disclosure Vulnerability
- CVE-2022-29122 Windows Clustered Shared Volume Information Disclosure Vulnerability
- CVE-2022-29121 Windows WLAN AutoConfig Service Denial of Service Vulnerability
- CVE-2022-29120 Windows Clustered Shared Volume Information Disclosure Vulnerability
- CVE-2022-29115 Windows Fax Service Remote Code Execution Vulnerability
- CVE-2022-29114 Windows Print Spooler Information Disclosure Vulnerability
- CVE-2022-29113 Windows Digital Media Receiver Elevation of Privilege Vulnerability
- CVE-2022-29112 Windows Graphics Component Information Disclosure Vulnerability

- CVE-2022-29106 Windows Hyper-V Shared Virtual Disk Elevation of Privilege Vulnerability
- CVE-2022-29105 Microsoft Windows Media Foundation Remote Code Execution Vulnerability
- CVE-2022-29104 Windows Print Spooler Elevation of Privilege Vulnerability
- CVE-2022-29103 Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
- CVE-2022-29102 Windows Failover Cluster Information Disclosure Vulnerability
- CVE-2022-26939 Storage Spaces Direct Elevation of Privilege Vulnerability
- CVE-2022-26938 Storage Spaces Direct Elevation of Privilege Vulnerability
- CVE-2022-26937 Windows Network File System Remote Code Execution Vulnerability
- CVE-2022-26936 Windows Server Service Information Disclosure Vulnerability
- CVE-2022-26935 Windows WLAN AutoConfig Service Information Disclosure Vulnerability
- CVE-2022-26934 Windows Graphics Component Information Disclosure Vulnerability
- CVE-2022-26933 Windows NTFS Information Disclosure Vulnerability
- CVE-2022-26932 Storage Spaces Direct Elevation of Privilege Vulnerability
- CVE-2022-26931 Windows Kerberos Elevation of Privilege Vulnerability
- CVE-2022-26930 Windows Remote Access Connection Manager Information Disclosure Vulnerability
- CVE-2022-26927 Windows Graphics Component Remote Code Execution Vulnerability
- CVE-2022-26926 Windows Address Book Remote Code Execution Vulnerability
- CVE-2022-26925 Windows LSA Spoofing Vulnerability
- CVE-2022-26923 Active Directory Domain Services Elevation of Privilege Vulnerability
- CVE-2022-26913 Windows Authentication Security Feature Bypass Vulnerability
- CVE-2022-26788 PowerShell Elevation of Privilege Vulnerability
- CVE-2022-24513 Visual Studio Elevation of Privilege Vulnerability
- CVE-2022-24466 Windows Hyper-V Security Feature Bypass Vulnerability
- CVE-2022-23270 Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
- CVE-2022-22019 Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2022-22016 Windows PlayToManager Elevation of Privilege Vulnerability
- CVE-2022-22015 Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability
- CVE-2022-22014 Windows LDAP Remote Code Execution Vulnerability
- CVE-2022-22013 Windows LDAP Remote Code Execution Vulnerability
- CVE-2022-22012 Windows LDAP Remote Code Execution Vulnerability
- CVE-2022-22011 Windows Graphics Component Information Disclosure Vulnerability
- CVE-2022-21972 Point-to-Point Tunneling Protocol Remote Code Execution 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:

| Product | OS | Hotfix | Download website | Pre-installed patch |
|---|---|---|---|---|
| BeneVision | Windows 10 | KB5013941 | https://catalog.s.download.windows | KB5005112 |

| | | | | |
|---|---|---|---|---|
| CMS | Professional SP1 64bit 1809 | | update.com/d/msdownload/update/software/secu/2022/05/windows10.0-kb5013941-x64_8df2c89490d6cd19f5086728dbc3c991decefad7.msu | KB5003243<br>KB4587735 |
| | Windows Server 2019 | KB5013941 | https://catalog.s.download.windowsupdate.com/d/msdownload/update/software/secu/2022/05/windows10.0-kb5013941-x64_8df2c89490d6cd19f5086728dbc3c991decefad7.msu | KB5005112<br>KB5003243<br>KB4587735 |
| | Windows 10 1607 for 32-bit | KB5013952 | https://catalog.s.download.windowsupdate.com/c/msdownload/update/software/secu/2022/05/windows10.0-kb5013952-x86_b2adf7f0b5163f0efc86cd13bc9fbb59b5ede70f.msu | KB4498947<br>KB4132216 |
| | Windows 10 1607 for x64-based | KB5013952 | https://catalog.s.download.windowsupdate.com/d/msdownload/update/software/secu/2022/05/windows10.0-kb5013952-x64_c9c29b4a81897db5545e284f04490c0659dc8b06.msu | KB4498947<br>KB4132216 |
| | Windows Server 2012 R2 | KB5014001 | https://catalog.s.download.windowsupdate.com/c/msdownload/update/software/secu/2022/04/windows8.1-kb5012639-x64_3a6168057b11b31200c4ad9eb7cd268829e7e3be.msu | |
| | Windows Server 2016 | KB5013952 | https://catalog.s.download.windowsupdate.com/d/msdownload/update/software/secu/2022/05/windows10.0-kb5013952-x64_c9c29b4a81897db5545e284f04490c0659dc8b06.msu | KB4498947<br>KB4132216 |
| BeneVision CMS Viewer | Windows 10 Professional SP1 64bit 1809 | KB5013941 | https://catalog.s.download.windowsupdate.com/d/msdownload/update/software/secu/2022/05/windows10.0-kb5013941-x64_8df2c89490d6cd19f5086728dbc3c991decefad7.msu | KB5005112<br>KB5003243<br>KB4587735 |
| | Windows 10 1607 for 32-bit | KB5013952 | https://catalog.s.download.windowsupdate.com/c/msdownload/update/software/secu/2022/05/windows10.0-kb5013952-x86_b2adf7f0b5163f0efc86cd13bc9fbb59b5ede70f.msu | KB4498947<br>KB4132216 |
| | Windows 10 1607 | KB5013952 | https://catalog.s.download.windows | KB4498947 |

| | | | | |
|---|---|---|---|---|
| | for x64-based | | update.com/d/msdownload/update/software/secu/2022/05/windows10.0-kb5013952-x64_c9c29b4a81897db5545e284f04490c0659dc8b06.msu | KB4132216 |
| | Windows Server 2012 R2 | KB5014011 | https://catalog.s.download.windowsupdate.com/c/msdownload/update/software/secu/2022/05/windows8.1-kb5014011-x64_8677efb857d5a370986406a2bf133ba4e1947f16.msu | |
| Hypervisor X CMS | Windows 10 Professional SP1 64bit 1809 | KB5013941 | https://catalog.s.download.windowsupdate.com/d/msdownload/update/software/secu/2022/05/windows10.0-kb5013941-x64_8df2c89490d6cd19f5086728dbc3c991decefad7.msu | KB5005112 KB5003243 KB4587735 |
| | Windows Server 2019 | KB5013941 | https://catalog.s.download.windowsupdate.com/d/msdownload/update/software/secu/2022/05/windows10.0-kb5013941-x64_8df2c89490d6cd19f5086728dbc3c991decefad7.msu | KB5005112 KB5003243 KB4587735 |
| | Windows 10 1607 for 32-bit Systems | KB5013952 | https://catalog.s.download.windowsupdate.com/c/msdownload/update/software/secu/2022/05/windows10.0-kb5013952-x86_b2adf7f0b5163f0efc86cd13bc9fbb59b5ede70f.msu | KB4498947 KB4132216 |
| | Windows 10 1607 for x64-based Systems | KB5013952 | https://catalog.s.download.windowsupdate.com/c/msdownload/update/software/secu/2022/05/windows10.0-kb5013952-x86_b2adf7f0b5163f0efc86cd13bc9fbb59b5ede70f.msu | KB4498947 KB4132216 |
| eGateway | Windows 10 Professional SP1 64bit 1809 | KB5013941 | https://catalog.s.download.windowsupdate.com/d/msdownload/update/software/secu/2022/05/windows10.0-kb5013941-x64_8df2c89490d6cd19f5086728dbc3c991decefad7.msu | KB5005112 KB5003243 KB4587735 |
| | Windows Server 2019 | KB5013941 | https://catalog.s.download.windowsupdate.com/d/msdownload/update/software/secu/2022/05/windows10.0-kb5013941-x64_8df2c89490d6cd19f5086728dbc3c991decefad7.msu | KB5005112 KB5003243 KB4587735 |
| | Windows 10 1607 | KB5013952 | https://catalog.s.download.windows | KB4498947 |

| | | | | |
|---|---|---|---|---|
| | for x64-based | | update.com/c/msdownload/update/software/secu/2022/05/windows10.0-kb5013952-x86_b2adf7f0b5163f0efc86cd13bc9fbb59b5ede70f.msu | KB4132216 |
| | Windows Server 2012 R2 | KB5014001 | https://catalog.s.download.windowsupdate.com/c/msdownload/update/software/secu/2022/04/windows8.1-kb5012639-x64_3a6168057b11b31200c4ad9eb7cd268829e7e3be.msu | |
| | Windows Server 2016 | KB5013952 | https://catalog.s.download.windowsupdate.com/d/msdownload/update/software/secu/2022/05/windows10.0-kb5013952-x64_c9c29b4a81897db5545e284f04490c0659dc8b06.msu | KB4498947<br>KB4132216 |
| MLDAP Server | Windows 10 1607 for x64-based | KB5013952 | https://catalog.s.download.windowsupdate.com/c/msdownload/update/software/secu/2022/05/windows10.0-kb5013952-x86_b2adf7f0b5163f0efc86cd13bc9fbb59b5ede70f.msu | KB4498947<br>KB4132216 |
| | Windows Server 2012 R2 | KB5014011 | https://catalog.s.download.windowsupdate.com/c/msdownload/update/software/secu/2022/05/windows8.1-kb5014011-x64_8677efb857d5a370986406a2bf133ba4e1947f16.msu | |
| | Windows Server 2016 | KB5013952 | https://catalog.s.download.windowsupdate.com/d/msdownload/update/software/secu/2022/05/windows10.0-kb5013952-x64_c9c29b4a81897db5545e284f04490c0659dc8b06.msu | KB4498947<br>KB4132216 |
| | Windows Server 2019 | KB5013941 | https://catalog.s.download.windowsupdate.com/d/msdownload/update/software/secu/2022/05/windows10.0-kb5013941-x64_8df2c89490d6cd19f5086728dbc3c991decefad7.msu | KB5005112<br>KB5003243<br>KB4587735 |
| BeneVision Mobile Server | Windows Server 2016 | KB5013952 | https://catalog.s.download.windowsupdate.com/c/msdownload/update/software/secu/2022/05/windows10.0-kb5013952-x86_b2adf7f0b5163f0efc86cd13bc9fbb59b5ede70f.msu | KB4498947<br>KB4132216 |
| | Windows Server | KB5014011 | https://catalog.s.download.windows | |

| | | | | |
|---|---|---|---|---|
| | 2012 R2 | | update.com/c/msdownload/update/software/secu/2022/05/windows8.1-kb5014011-x64_8677efb857d5a370986406a2bf133ba4e1947f16.msu | |
| | Windows Server 2019 | KB5013941 | https://catalog.s.download.windowsupdate.com/d/msdownload/update/software/secu/2022/05/windows10.0-kb5013941-x64_8df2c89490d6cd19f5086728dbc3c991decefad7.msu | KB5005112<br>KB5003243<br>KB4587735 |
| iView | Windows 10 1607 for x64-based | KB5013952 | https://catalog.s.download.windowsupdate.com/c/msdownload/update/software/secu/2022/05/windows10.0-kb5013952-x86_b2adf7f0b5163f0efc86cd13bc9fbb59b5ede70f.msu | KB4498947<br>KB4132216 |

## 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：2022-6-28