Mindray Patient Monitor/Anesthesia Cybersecurity Brief TLStorm 2.0

mindray
NORTH AMERICA

Intellectual Property Statement

Manufacturer's Responsibility

Contents of this document are subject to change without prior notice.

All information contained in this document is believed to be correct. Mindray shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

Background

On May 3, 2022, Armis Research published a report called TLStorm 2.0 (https://www.armis.com/blog/tlstorm-2-nanossl-tls-library-misuse-leads-to-vulnerabilities-in-common-switches/). Armis has discovered five vulnerabilities in the implementation of TLS communications in multiple models of Aruba and Avaya switches. Both vendors have been found to have switches vulnerable to remote code execution (RCE) vulnerabilities that can be exploited over the network. The exploitation of these RCE vulnerabilities can lead to:

- Breaking of network segmentation, allowing lateral movement to additional devices by changing the behavior of the switch
- Data exfiltration of corporate network traffic or sensitive information from the internal network to the Internet
- Captive portal escape

CVE	Affected Component	Potential Impact
CVE-2022-23676	Aruba 5400R Series, Aruba 3810 Series, Aruba 2920 Series, Aruba 2930F Series, Aruba 2930M Series, Aruba 2530 Series, Aruba 2540 Series	RCE (remote code execution)
CVE-2022-23677	Aruba 5400R Series, Aruba 3810 Series, Aruba 2920 Series, Aruba 2930F Series, Aruba 2930M Series, Aruba 2530 Series, Aruba 2540 Series	RCE (remote code execution)
CVE-2022-29860	Avaya ERS3500 Series, Avaya ERS3600 Series, Avaya ERS4900 Series, Avaya ERS5900 Series	RCE (remote code execution)
CVE-2022-29861	Avaya ERS3500 Series, Avaya ERS3600 Series, Avaya ERS4900 Series, Avaya ERS5900 Series	RCE (remote code execution)
/	No assigned CVE as this is a discontinued product line from Avaya	RCE (remote code execution)

Mindray Course of Action

Mindray utilizes the Aruba 2930F series, as well as in some instances the Aruba 3810m network switches in the deployment of the Mindray biomedical device network. We do not use Avaya switches.

The Aruba 2930F/3810m switches used are potentially exposed by vulnerabilities CVE-2022-23677 and CVE-2022-23676. These vulnerabilities can be exploited only when the RAIDUS function on the switch has been enabled and has connected to an attacker-controlled RADIUS Server. Within the Mindray biomedical network, the RADIUS functions are disabled and Mindray does not enable or utilize this function at any Mindray installation, therefore TLStorm 2.0 will not impact the Aruba 2930F/3810m switches installed by Mindray.

Although there is no exposure to CVE-2022-23677 and CVE-2022-23676 for the Mindray system, Mindray will verify and release the updated Aruba firmware which addresses these vulnerabilities in a future software release.