Mindray Patient Monitor/Anesthesia Cybersecurity Brief Nucleus13

mindray
NORTH AMERICA

Intellectual Property Statement

mindray , MINDRAY and MINDRAY are the trademarks, registered or otherwise, of Mindray in China and other countries. All other trademarks that appear in this document are used only for informational or editorial purposes. They are the property of their respective owners.

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 November 9, 2021, Forescout Research published a report called NUCLEUS:13. (https://www.forescout.com/resources/nucleus13-research-report-dissecting-the-nucleus-tcpip-stack). The report details research they conducted into the Nucleus NET, the TCP/IP stack of the Siemens owned Nucleus real-time operating system (RTOS), where they found 13 new vulnerabilities.. These vulnerabilities will cause security risks to devices using the Nucleus RTOS.

CVE	Affected Component	Potential Impact
CVE-2021-31886	FTP Server	RCE
CVE-2021-31884	DHCP Client	DoS, Out-of-bound reads/writes. Impact depends on how the client is implemented.
CVE-2021-31887	FTP Server	RCE
CVE-2021-31888	FTP Server	RCE
CVE-2021-31346	IP/ICMP	Information leak/DoS
CVE-2021-31889	TCP Server	DoS
CVE-2021-31890	TCP Server	DoS
CVE-2021-31885	TFTP Server	Information Leak
CVE-2021-31345	UDP	DoS, Information leak. Impact depends on how UDP is implemented.
CVE-2021-31881	DHCP Client	DoS
CVE-2021-31883	DHCP Client	DoS
CVE-2021-31882	DHCP Client	DoS
CVE-2021-31344	ICMP	Confused Deputy

Mindray Course of Action

Mindray has investigated and subsequently determined that the Passport V, DPM 5/6/7, DPM+. TEL100 Receiver, TEL200 Receiver, Passport 12m/17m, ASeries A3/A4/A5/A7, TD60 Receiver, and Accutorr V products can potentially be impacted by a subset of these vulnerabilities.

CVE-2021-31885, CVE-2021-31886, CVE-2021-31887, CVE-2021-31888 are related to FTP/TFTP which is not used in any Mindray devices so these vulnerabilities do not impact the products listed above.

While overall risk is low due to inherent system design mitigations already in place (per common installation guidelines) Mindray has proceeded with addressing these vulnerabilities in products which are not at end of service life.

If you have any additional questions or are interested in reviewing further options to safeguard your Mindray patient monitoring platforms, please call Mindray Technical Support at 877-913-9663 (Option 1), 8:30 am – 5:30 pm ET.

Additionally, you may contact your local Sales Representative for an opportunity to discuss appropriate upgrade paths to bring any legacy systems up to their most current revisions.