POLSINELLI

Publications

February 11, 2025 • Updates

CISA and FDA Sound Alarm on Backdoor Cybersecurity Threat with Patient Monitoring Devices

Last week, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the U.S. Food and Drug Administration (FDA) released warnings about an embedded function they found in the firmware of the Contec CMS8000, which is a patient monitoring device used to provide continuous monitoring of a patient's vital signs, including electrocardiogram, heart rate, temperature, blood oxygen and blood pressure.[1] Health care organizations utilizing this device should take immediate action to mitigate the risk of unauthorized access to patient data, to determine whether or not such unauthorized access has already occurred, and to prevent future unauthorized access.

Contec Medical Systems (Contec), a global medical device and health care solutions company headquartered in China, sells medical equipment used in hospitals and clinics in the United States. The Contac CMS800 has also been re-labeled and sold by resellers, such as with the Epsimed MN-120.

The three cyber security vulnerabilities identified by CISA and FDA include:

- An unauthorized user may remotely control or modify the Contec CMS8000, and it may not work as intended.
- The software on the Contec CMS8000 includes a "backdoor," which allows the device or network to which the device has been connected to be compromised.
- The Contec CMS8000, once connected to the internet, will transmit the patient data it collects, including personally identifiable information (PII) and protected health information (PHI), to China.

Mitigation Strategies

Health care organizations should take an immediate inventory of their patient monitoring systems and determine whether their enterprise uses any of the impacted devices. Because there is no patch currently available, FDA recommends disabling all remote monitoring functions by unplugging the ethernet cable and disabling Wi-Fi or cellular connections if used. FDA further recommends that the devices in question be used only for local in-person monitoring. Per the FDA, if a health care provider needs remote monitoring, a different patient monitoring device from a different manufacturer should be

Related People

- Michael M. Gaba
- ILIANA L. PETERS
- Suzanne E. Bassett

Related Capabilities

- Food, Drug & Device
- Medical Devices
- HIPAA/Health Information Privacy & Security

used.

Health care providers that are not using impacted devices should still take the time to conduct an audit of their patient monitoring and other internet-connected devices to determine the risk of potential security breaches. Organizations should use this opportunity to evaluate, once again, their incident response plans, continue to conduct periodic risk assessments of their technologies, and evaluate whether their organization's policies, procedures, and plans enable them to fulfill cybersecurity requirements.[2] If you have any legal questions regarding impacted devices or how to mitigate the cybersecurity risks associated with this notice, please reach out to Michael Gaba, Iliana Peters or Suzanne Bassett.

[1] *See* CISA, Contec CMS800 Contains a Backdoor (January 30, 2025); FDA, Cybersecurity Vulnerabilities with Certain Patient Monitors from Contec and Epsimed: FDA Safety Communication (January 30, 2025).

[2] *See e.g.,* Polsinelli's discussion of cybersecurity compliance in 2025.