Cybersecurity Vulnerabilities with Certain Patient Monitors from Contec and Epsimed: FDA Safety Communication

Date Issued: January 30, 2025

The U.S. Food and Drug Administration (FDA) is raising awareness among health care providers, health care facilities, patients, and caregivers that cybersecurity vulnerabilities in Contec CMS8000 patient monitors and Epsimed MN-120 patient monitors (which are Contec CMS8000 patient monitors relabeled as MN-120) may put patients at risk after being connected to the internet.

Three cybersecurity vulnerabilities have been identified:

- The patient monitor may be remotely controlled by an unauthorized user or not work as intended.
- The software on the patient monitors includes a backdoor, which may mean that the device or the network to which the device has been connected may have been or could be compromised.
- Once the patient monitor is connected to the internet, it begins gathering patient data, including personally identifiable information (PII) and protected health information (PHI), and exfiltrating (withdrawing) the data outside of the health care delivery environment.

These cybersecurity vulnerabilities can allow unauthorized actors to bypass cybersecurity controls, gaining access to and potentially manipulating the device.

The FDA is not aware of any cybersecurity incidents, injuries, or deaths related to these cybersecurity vulnerabilities at this time.

Recommendations for Patients and Caregivers

- Talk to your health care provider about whether your device relies on remote monitoring features. Remote monitoring means the device uses an internet connection to allow a health care provider to evaluate patient vital signs from another location (such as a remote monitoring system or central monitoring system).
    - If your health care provider confirms that your device relies on remote monitoring features, unplug the device and stop using it. Talk to your health

care provider about finding an alternative patient monitor.

- If your device does not rely on remote monitoring features, use only the local monitoring features of the patient monitor. This means unplugging the device's ethernet cable and disabling wireless (that is, WiFi or cellular) capabilities, so that patient vital signs are only observed by a caregiver or health care provider in the physical presence of a patient.
  - If you cannot disable the wireless capabilities, unplug the device and stop using it. Talk to your health care provider about finding an alternative patient monitor.

- Be aware the FDA is not aware of any cybersecurity incidents, injuries, or deaths related to this vulnerability at this time.
- Report any problems or complications with your Contec CMS8000 patient monitor or Epsimed MN-120 patient monitor to the FDA.

Recommendations for Health Care Providers

- Work with health care facility staff to determine if a patient's Contec CMS8000 patient monitor or Epsimed MN-120 patient monitor may be affected and how to reduce any associated risk.
- Read and follow the recommendations for patients and caregivers in this safety communication.
- Check the Contec CMS8000 patient monitors and Epsimed MN-120 patient monitors for any signs of unusual functioning, such as inconsistencies between the displayed patient vitals and the patient's actual physical state.
- Report any problems with your Contec CMS8000 patient monitor or Epsimed MN-120 patient monitor to the FDA.

Recommendations for Health Care Facility Staff (including Information Technology (IT) and Cybersecurity Staff)

- **Use only the local monitoring features of the device.**
  - If your patient monitor relies on remote monitoring features, unplug the device and stop using it.
  - If your device **does not** rely on remote monitoring features, unplug the device's ethernet cable and disable wireless (that is, WiFi or cellular) capabilities. If you cannot disable the wireless capabilities, then continuing to

use the device will expose the device to the backdoor and possible continued patient data exfiltration.

- Review the Cybersecurity and Infrastructure Security Agency (CISA) "Mitigations" section (https://www.cisa.gov/news-events/ics-medical-advisories/icsma-25-030-01) in the vulnerabilities related advisory.
- Be aware, at this time there is no software patch available to help mitigate this risk.
- Check the Contec CMS8000 patient monitors and Epsimed MN-120 patient monitors for any signs of unusual functioning, such as inconsistencies between the displayed patient vitals and the patient's actual physical state.
- Report any problems with your Contec CMS8000 patient monitor or Epsimed MN-120 patient monitor to the FDA.

Device Description

Patient monitors are used in health care and home settings for displaying information, such as the vital signs of a patient, including temperature, heartbeat, and blood pressure.

Cybersecurity Vulnerabilities May Affect Contec CMS8000 and Epsimed MN-120 Patient Monitors

Three cybersecurity vulnerabilities have been identified, whose potential impacts fall into two main categories. A vulnerable device could be exploited to:

- Deny access to the device, such as cause the device to crash and be unable to work as intended.
- Take over the device to remotely control it to perform unexpected or undesired actions, such as corrupting the data.

The vulnerabilities could allow all vulnerable Contec and Epsimed patient monitors on a given network to be exploited at the same time.

Additionally, the software on the patient monitors includes a backdoor. "Backdoor" is the term used to describe hidden functionality that device users are not told about and can allow unauthorized actors to bypass cybersecurity controls. The unauthorized actors could access and potentially manipulate the device. Given the backdoor, the device and/or the network to which the device has been connected may have been or could be compromised.

Also, the FDA has authorized these patient monitors only for wired functionality (that is, ethernet connectivity). However, the FDA is aware that some patient monitors may be

available with wireless (that is, WiFi or cellular) capabilities without FDA authorization.

The Cybersecurity and Infrastructure Security Agency (CISA) has identified that once the patient monitor is connected to the internet, it begins gathering and exfiltrating (withdrawing) patient data outside of the health care delivery environment, including when the device is used in a home setting. The FDA and CISA continue to work with Contec to correct these vulnerabilities as soon as possible.

Unique Device Identifier (UDI)

The unique device identifier helps identify individual medical devices, including patient monitors, sold in the United States from manufacturing through distribution to patient use. The UDI allows for more accurate reporting, reviewing, and analyzing of adverse event reports so that devices can be identified, and problems potentially corrected more quickly.

- How do I recognize a UDI on a label? (https://www.fda.gov/medical-devices/unique-device-identification-system-udi-system/udi-basics#recognize)
- AccessGUDID database - Identify Your Medical Device (https://accessgudid.nlm.nih.gov/)
- Benefits of a UDI System (/medical-devices/unique-device-identification-system-udi-system/benefits-udi-system)

You can identify the devices affected by checking the unique device identifier (UDI), which is a unique numeric or alphanumeric code that generally includes a device identifier (DI) that identifies the labeler and the specific version or model of a device.

Brand Name	Version or Model	UDI-DI
Contec	CMS8000	06945040100034
Epsimed	MN-120	N/A

FDA Actions

The FDA takes seriously any reports of cybersecurity vulnerabilities in medical devices and will continue to work with Contec and CISA to correct these vulnerabilities as soon as possible.

The FDA will continue to assess new information concerning the vulnerabilities and will keep the public informed if significant new information becomes available.

Read more about medical device cybersecurity. (/medical-devices/digital-health-center-

excellence/cybersecurity)

Reporting Problems with Your Device

If you think you had a problem with a Contec CMS8000 or Epsimed MN-120 patient monitors, the FDA encourages you to report the problem through the MedWatch Voluntary Reporting Form (https://www.accessdata.fda.gov/scripts/medwatch/index.cfm?action=reporting.home).

Health care personnel employed by facilities that are subject to the FDA's user facility reporting requirements should follow the reporting procedures established by their facilities.

Questions?

If you have questions, contact CDRH's Division of Industry and Consumer Education (DICE) (/medical-devices/device-advice-comprehensive-regulatory-assistance/contact-us-division-industry-and-consumer-education-dice).