Field Safety Notification

FSN-CMS8000

Brand name	Contec	**Model and Product Name**	CMS8000 Patient Monitor
SN/LOT	See the attachment	**Date**	2025/02/10

Problem Description:

Recently, our company have known from FDA and CISA that the CMS8000 patient monitor has the following cybersecurity vulnerabilities:

1.The patient monitor may be remotely controlled by an unauthorized user or not work as intended.

2.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.

3.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.

To date, Contec is not aware of are not aware of any cybersecurity incidents, injuries, or deaths related to these cybersecurity vulnerabilities at this time.

However, considering that these cybersecurity vulnerabilities may put patients at risk when the patient monitor is connected to the Internet, in accordance with the EU MDR regulations and the company's relevant control procedures, we issue this Field Safety Notice (FSN).

Impact:

The CMS8000 patient monitor is intended to be used for monitoring, displaying, reviewing, storing, and alarming of multiple physiological parameters including ECG, heart rate, respiration rate, non-invasive blood pressure, invasive blood pressure, carbon dioxide and temperature of adult, pediatric and neonatal patients. If the vulnerability is exploited, it could lead to the following:

- Disruption of the continuous monitoring of vital signs, leading to delay in the detection of critical changes in a patient’s health condition and delayed medical intervention.
- Manipulation or corruption of data being transmitted by the patient monitor leading to incorrect readings and potentially harmful medical decisions based on false data.

For who have received this notice and are determined to be affected by this vulnerability, please take the following mitigation actions:

1.If the user's device is currently in stand-alone use and there are no plans to connect it to any network (including wired or wireless networks), the user can temporarily postpone this update. However, once there are plans to connect the device to a network in the future, please promptly download the software upgrade package sent by our company and install it according to the software upgrade guide to ensure the cybersecurity.

2.If the user's device is in a closed local area network (LAN) that is physically isolated from the Internet and no other devices except medical devices are connected to this network, the network security risk in such a environment is extremely low. In this case, the user can decide whether to download and install the software upgrade package according to the actual situation. If there are plans to connect the device to a non-closed private network in the future, please promptly download the software upgrade package sent by our company and install it according to the software upgrade guide to ensure the cybersecurity.

3.If the user's device is not used in a secure network environment (i.e., not in a closed local area network (LAN) that is physically isolated from the Internet and with no other devices except medical devices connected to the network), please take the following immediate and long-term actions:
a. Immediate actions: It is recommended to take the measure of safely disconnecting from the network by unplugging the network cable and only enabling the local monitoring function.
b. Long-term mitigation actions: Please promptly download the software upgrade package sent by our company and install it according to the software upgrade guide to ensure the cybersecurity.

How to Identify Affected Products:

Please check the SN of the device used and the attachment “Affected Product Information”. If your used device is in this attachment, it is the affected device.
Please refer to the attachment: Affected Product Information.

Contact Information:

If you have any questions, please do not hesitate to let us know by email. E-mail: contec_monitor@contecmed.com. We will get back to you promptly and work with you to resolve the issue.

Note：

This Field Safety Notification should be shared with anyone who needs to be aware within your organization and forwarded to any organization where potentially affected devices have been transferred.

Drafted by: Xiao Jie

Approved by():Yang Zhishan (General Manager) signature:

Contec Medical Systems Co., Ltd.
Date:2025-2-10