

Cybersecurity Vulnerabilities in Certain GE Healthcare Clinical Information Central Stations and Telemetry Servers: Safety Communication

Date Issued: January 23, 2020

The U.S. Food and Drug Administration (FDA) is raising awareness among health care providers and facility staff that cybersecurity vulnerabilities in certain GE Healthcare Clinical Information Central Stations and Telemetry Servers may introduce risks to patients while being monitored.

These devices are used mostly in health care facilities for displaying information, such as the physiologic parameters of a patient (such as temperature, heartbeat, blood pressure), and monitoring patient status from a central location in a facility, such as a nurse's workstation. To date, the FDA is not aware of any adverse events related to these vulnerabilities. Learn more about these vulnerabilities


On November 12, 2019, GE Healthcare issued an "Urgent Medical Device Correction" letter informing consumers of security vulnerabilities for certain GE Healthcare Clinical Information Central Stations and Telemetry Servers, instructions for risk mitigation, and where to find the software updates or patches when they become available. The following table provides information on the specific versions of the devices that have these security vulnerabilities.

DEVICE	SOFTWARE VERSION	RECALL INFORMATION
ApexPro Telemetry Server and CARESCAPE Telemetry Server	4.2 and earlier	ApexPro (https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfRES/res.cfm?id=178163), CARESCAPE (https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfres/res.cfm?id=178167)
CARESCAPE Central Station (CSCS) version 1	1.x	CARESCAPE (https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfres/res.cfm?id=178167)
CIC Pro Clinical Information Center Central Station version 1	4.x, 5.x	Central Information Center (CIC) (https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfRES/res.cfm?id=178165)

Recommendations for Health Care Providers

- Work with health care facility staff to determine if a medical device used by a patients may be affected and how to reduce associated risk.

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

- GE Healthcare will be issuing a software patch to address the vulnerabilities and will notify affected customers to deploy them when the patches are ready. Information about the patches will be posted on the GE Healthcare product security portal (<https://securityupdate.gehealthcare.com/>)  (<http://www.fda.gov/about-fda/website-policies/website-disclaimer>).
- The risk posed by the vulnerabilities can be reduced by segregating the network connecting the patient monitors with the GE Healthcare Clinical Information Central Stations and Telemetry Servers from the rest of the hospital network, as described in the GE Healthcare documentation for these devices.
- Use firewalls, segregated networks, virtual private networks, network monitors, or other technologies that minimize the risk of remote or local network attacks.

Recommendations for Patients and Caregivers

- Talk with your health care provider if you have any concerns. The FDA is not aware of any adverse events related to this vulnerability.


Cybersecurity Vulnerabilities

A security firm has identified several vulnerabilities in certain GE Healthcare Clinical Information Central Stations and Telemetry Servers, that may allow an attacker to remotely take control of the medical device and to silence alarms, generate false alarms and interfere with alarms of patient monitors connected to these devices.

Health care providers use GE Clinical Information Central Stations and Telemetry Servers to collect and display data from multiple patient monitoring devices. The data includes physiological status (such as temperature, heartbeat, blood pressure), patient demographic or other nonmedical information.

These vulnerabilities might allow an attack to happen undetected and without user interaction. Because an attack may be interpreted by the affected device as normal network communications, it may remain invisible to existing security measures.

For more information about these vulnerabilities see:

- Department of Homeland Security Cybersecurity Infrastructure Security Advisory (<https://www.us-cert.gov/ics/advisories/icsma-20-023-01>)
- GE Healthcare Guidance on the Cybersecurity vulnerability (<https://www.gehealthcare.com/security>)  (<http://www.fda.gov/about-fda/website-policies/website-disclaimer>)

FDA Actions

The FDA takes reports of cybersecurity vulnerabilities in medical devices seriously and will continue to work with GE Healthcare as the firm develops software patches 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 (<https://www.fda.gov/medical-devices/digital-health/cybersecurity>)

Reporting Problems with Your Device

If you think you had a problem with your device or a device your patient uses, 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, email the Division of Industry and Consumer Education (DICE) at DICE@FDA.HHS.GOV (<mailto:DICE@FDA.HHS.GOV>) or call 800-638-2041 or 301-796-7100 .