URGENT FIELD SAFETY NOTICE

GE Healthcare
3000 N. Grandview Blvd. - W440
Waukesha, WI 53188, USA

<Date of Letter Deployment>

GEHC Ref# 36142

To: Director of Biomedical / Clinical Engineering
Chief Information Security Officer
Health Care Administrator / Risk Manager

RE: **Security vulnerability of certain GE Central Stations and ApexPro Telemetry servers**

This document contains important information for your product. Please ensure that all potential users in your facility are made aware of this safety notification and the recommended actions. Please retain this document for your records.

Safety Issue

When connected to the Mission Critical (MC) and /or Information Exchange (IX) networks, certain versions of the CARESCAPE Telemetry Server, Apex Telemetry Server, CARESCAPE Central Station (CSCS) version 1 and Central Information Center (CIC) systems were identified to have vulnerabilities to a cyber-attack.

The MC and IX networks are isolated from other hospital networks and traffic. As a result, for this issue to occur, the unauthorized person would need to gain physical access to the monitoring devices themselves or acquire direct access to the isolated MC or IX networks on-site at the hospital.

If an unauthorized person with special skills gains this level of access, a combination of an exposed private key, exposed services, and components with identified software vulnerabilities could potentially be exploited and combined with further targeted malicious action to:

- Make changes at the operating system level of the device with effects such as rendering the device unusable, and/or
- Utilize services used for remote viewing and control of devices on the network to access the clinical user interface and make changes to device settings and alarm limits.

In this situation, such cyber-attacks could possibly result in a loss of monitoring and/or loss of alarms during active patient monitoring.

There have been no reported incidences in a clinical use setting of such a cyber-attack occurring, or any reported injuries as a result of this issue.

Safety Instructions

You can continue to use your product. Please follow Patient Monitoring Network Configuration Guide, CARESCAPE Network Configuration Guide and your product Technical and Service Manuals for information on proper configuration of the patient monitor networks.

In addition to applying network management best practices, ensure:

1. MC and IX Networks are isolated;

2. MC and IX Router/Firewalls block incoming traffic, as applicable;
3. Restricted physical access to Central Stations, Telemetry Servers, MC network and IX network;
4. Default passwords are changed as applicable; and
5. Password management best practices are adhered to

Ensuring the networks are properly configured and isolated protects against these potential concerns and mitigates the risk.

Continual Cybersecurity Hygiene

As part of continual cybersecurity hygiene updates, GE develops software updates/patches that include security enhancements. Customers can access GE's security website (https://securityupdate.gehealthcare.com) to receive the most up to date information, and can subscribe to receive notifications when new updates/patches are available.

Please keep this notification with your manuals for future reference.

Affected Product Details

Please see the table below to identify the affected products. Identification numbers are located on the product label affixed to the back of the unit. Identify the affected product by locating the 9-, 10-, 11- or 13- digit GE Healthcare serial number.

Product codes by Product:

Product	Product Code
Telemetry Servers	GU, 3F, 4T, SAH, SEE
Central Stations	JA1, SCH, EF, 4T, AA1, GX, GQ, GU, SDY, SDZ, SGL, SGJ, SGK

Server Serial Number: 13 Digit	Server Serial Number: 9, 10, or 11 Digit
XXX XX XX XXXX XX Three-digit product code identifier	XX XX XXXX X XX Two-digit product code identifier

Contact Information

If you have any questions or concerns regarding this notification, please contact GE Healthcare Service or your local Service Representative. Please complete and return the attached "Customer Response" form via e-mail to Recall.36142@ge.com.

GE Healthcare confirms that this notice has been notified to the appropriate Regulatory Agency.

Please be assured that maintaining a high level of safety and quality is our highest priority. GE Healthcare provides security related information and patches via https://securityupdate.gehealthcare.com to assist you in keeping your product software current. If you have any questions, please contact us immediately per the contact information above.

Sincerely,

Laila Gurney
Senior Executive, Quality & Regulatory
GE Healthcare

Jeff Hersh, PhD MD
Chief Medical Officer
GE Healthcare

GE Healthcare

GEHC Ref# 36142

MEDICAL DEVICE NOTIFICATION ACKNOWLEDGEMENT
RESPONSE REQUIRED

Please complete this form and return it to GE Healthcare promptly upon receipt and no later than 30 days from receipt. This will confirm receipt and understanding of the Medical Device Correction Notice Ref# 36142.

Customer/Consignee Name: _____

Street Address: _____

City/State/ZIP/Country: _____

Email Address: _____

Phone Number: _____

☐ We acknowledge receipt and understanding of the accompanying Medical Device Notification, and that we have informed appropriate staff and have taken and will take appropriate actions in accordance with that Notification.

Please provide the name of the individual with responsibility who has completed this form.

Signature: _____

Printed Name: _____

Title: _____

Date (DD/MM/YYYY): _____

Please return completed form by scanning or taking a photo of the completed form and e-mailing to:
Recall.36142@ge.com

You may obtain this e-mail address through the QR code below: