



DRINGENDE SICHERHEITSINFORMATION

GE Healthcare

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

Interne GE Healthcare Ref.-Nr.: FMI 36142

27. Jänner 2020

An: Beauftragter für Medizinproduktesicherheit
Leitung der Medizintechnik
Leitender Verantwortlicher für Informationssicherheit
Klinikverwaltung / Gesundheitswesen

Betreff: **Sicherheitsrisiko für bestimmte GE-Zentralstationen und ApexPro Telemetrieserver**

Dieses Dokument enthält wichtige Informationen in Bezug auf Ihr Produkt. Bitte sorgen Sie dafür, dass alle potenziellen Anwender in Ihrer Einrichtung auf diese Sicherheitsmitteilung und die empfohlenen Maßnahmen hingewiesen werden. Bitte bewahren Sie dieses Dokument für Ihre Unterlagen auf.

Sicherheits- problem

Es wurde festgestellt, dass bestimmte Versionen des CARESCAPE Telemetrieservers, Apex Telemetrieservers, der CARESCAPE Zentralstation (CSCS) Version 1 und der Central Information Center (CIC)-Systeme Schwachstellen besitzen, die sie bei Verbindung mit dem Mission Critical (MC)- und/oder dem Information Exchange (IX)- Netzwerk anfällig für Cyberangriffe machen.

Die MC- und IX-Netzwerke sind von anderen Krankenhausnetzwerken und vom Datenverkehr isoliert. Damit dieses Problem auftreten kann, müsste die unbefugte Person daher physischen Zugang zu den Überwachungsgeräten selbst oder direkten Zugriff auf die isolierten MC- oder IX-Netzwerken vor Ort im Krankenhaus erhalten.

Wenn eine unbefugte Person mit Spezialkenntnissen einen solchen Zugriff erhält, könnte eine Kombination aus einem offengelegten privaten Schlüssel, anfälligen Diensten und Komponenten mit identifizierten Softwareschwachstellen potenziell ausgenutzt und dies mit weiteren gezielten böswilligen Aktionen kombiniert werden, um Folgendes durchzuführen:

- Veränderungen auf Betriebssystemebene des Geräts vornehmen, wodurch das Gerät z. B. unbrauchbar wird, und/oder
- Dienste, die zur Fernüberwachung und -steuerung von Geräten im Netzwerk dienen, für den Zugriff auf die klinische Benutzeroberfläche nutzen, um Änderungen an den Geräteeinstellungen und Alarmgrenzen vorzunehmen.

In einer solchen Situation könnten derartige Cyberangriffe möglicherweise zu einer verminderten Überwachung und/oder Verringerung von Alarmen während der aktiven Patientenüberwachung führen.

Es wurden bisher keine derartigen Vorfälle mit Cyberangriffen in klinischen Einrichtungen oder Verletzungen aufgrund dieses Problems gemeldet.

Vorsichts- maßnahmen

Sie können Ihr Produkt normal weiter verwenden. Bitte befolgen Sie die Anweisungen zur korrekten Konfiguration der Patientenüberwachungsnetzwerke, die in der Konfigurationsanleitung des Patientenüberwachungsnetzwerks, der Konfigurationsanleitung des CARESCAPE-Netzwerks und den technischen und Wartungshandbüchern Ihrer Geräte aufgeführt sind.

Wenden Sie stets die bewährten Vorgehensweisen für das Netzwerkmanagement an und sorgen Sie außerdem dafür, dass

1. MC- und IX-Netzwerke isoliert sind
2. MC- und IX-Router bzw. -Firewalls den eingehenden Verkehr blockieren (soweit zutreffend)
3. der physische Zugang zu Zentralstationen, Telemetrieservern, dem MC-Netzwerk und dem IX-Netzwerk beschränkt ist

4. Standard-Passwörter geändert werden, soweit zutreffend, und
5. beim Passwort-Management die bewährten Vorgehensweisen befolgt werden.

Die Sorge dafür, dass die Netzwerke richtig konfiguriert und isoliert sind, schützt vor diesen potenziellen Problemen und mindert das Risiko.

Betroffene Produkte

Im Rahmen kontinuierlicher Aktualisierungen zur Cybersicherheitshygiene entwickelt GE Software-Updates/-Patches, die Sicherheitsverbesserungen beinhalten. Unsere Kunden können die Sicherheits-Website von GE (<https://securityupdate.gehealthcare.com>) besuchen, um die neuesten Informationen zu erhalten. Dort können sie sich ebenfalls anmelden, um Benachrichtigungen zu erhalten, wenn neue Updates/Patches verfügbar sind.

Bitte bewahren Sie diese Benachrichtigung zusammen mit Ihren Handbüchern zu Referenzzwecken auf.

Korrekturmaßnahmen am System

Bitte beachten Sie die folgende Tabelle, um die betroffenen Produkte zu identifizieren. Die Identifikationsnummern befinden sich auf dem auf der Rückseite des Gerätes angebrachten Produktetikett. Identifizieren Sie das betroffene Produkt mithilfe der 9-, 10-, 11- oder 13-stelligen Seriennummer von GE Healthcare.

Produkt-Codes nach Produkt:

Produkt	Produkt-Code
Telemetrieserver	GU, 3F, 4T, SAH, SEE
Zentralstationen	JA1, SCH, EF, 4T, AA1, GX, GQ, GU, SDY, SDZ, SGL, SGJ, SGK

Server-Seriennummer: 13-stellig	Server-Seriennummer: 9-, 10- oder 11-stellig
XXX XX XX XXXX XX	XX XX XXXX X XX
Dreistellige Produkt-Code-Kennung	Zweistellige Produkt-Code-Kennung

Ansprechpartner

Bei Fragen zu dieser Korrekturmaßnahme oder zur Identifikation der betroffenen Produkte wenden Sie sich bitte an Ihren lokalen Vertriebs- oder Servicerepräsentanten oder an das Service Center unseres Technischen Kundendienstes.

Deutschland:
 T: 0800 4343 258
 F: 0800 5894315220
 E: FMI.Germany@ge.com

Schweiz/Liechtenstein:
 Anandic Medical Systems AG
 T: +41(0)848 800 950
 F: +41 (0)52 646 03 03
 E: info@anandic.com

Österreich:
 Sanitas GmbH
 T: +43 (0)662 852 186-0
 F: +43 (0)662 852 186-70
 E: sanitas@sanitas.at

Belgien/Luxemburg:
 Acertys
 T +32 (0)3 870 11 11
 F +32 (0)3 870 11 12
 E: info.be@acertys.com

GE Healthcare bestätigt, dass diese Mitteilung an die zuständige nationale Behörde übermittelt wurde.

Wir möchten in diesem Zusammenhang betonen, dass die Aufrechterhaltung eines hohen Sicherheits- und Qualitätsniveaus unsere vorrangige Priorität darstellt. Bitte wenden Sie sich umgehend an uns, falls Sie irgendwelche Zweifel haben.

Mit freundlichen Grüßen,



Laila Gurney
Senior Executive, Global Regulatory and Quality
GE Healthcare



Jeff Hersh, PhD MD
Chief Medical Officer
GE Healthcare



GE Healthcare

GEHC Ref. 36142

**BESTÄTIGUNG DER MITTEILUNG ÜBER MEDIZINISCHE GERÄTE
ANTWORT ERFORDERLICH**

Bitte füllen Sie dieses Formular aus und senden Sie es umgehend nach Erhalt, spätestens jedoch innerhalb von 30 Tagen nach Erhalt, an GE Healthcare zurück. Dadurch bestätigen Sie, dass Sie die Mitteilung zu der Korrekturmaßnahme für medizinische Geräte, Ref-Nr. 36142, erhalten und verstanden haben.

Name des Kunden/Warenempfängers: _____

Straße: _____

Ort/Bundesland/PLZ/Land: _____

E-Mail-Adresse: _____

Telefonnummer: _____

- Wir bestätigen den Erhalt und die Kenntnisnahme der beigegeführten Mitteilung über Medizinprodukte und bestätigen ebenfalls, dass wir die zuständigen Mitarbeiter informiert haben und in Übereinstimmung mit dieser Mitteilung geeignete Maßnahmen ergriffen haben und ergreifen werden.

Bitte geben Sie den Namen der zuständigen Person an, die dieses Formular ausgefüllt hat.

Unterschrift: _____

Titel: _____

Datum (TT/MM/JJJJ): _____

Bitte senden Sie das ausgefüllte Formular gescannt oder als Foto per E-Mail an:

FMI@anandic.com