URGENTE VEILIGHEIDSMEDEDELING

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

GE Healthcare ref.: FMI 36142

27 januari 2020

Aan: Directeur biomedische/klinische techniek
Hoofdfunctionaris Informatiebeveiliging
Gezondheidszorgbeheerder/risicomanager

Betreft: **Beveiligingskwetsbaarheid van bepaalde GE Central Stations en ApexPro Telemetrie-servers**

Dit document bevat belangrijke informatie voor uw product. Zorg ervoor dat alle mogelijke gebruikers in uw instelling op de hoogte worden gesteld van dit veiligheidsbericht en de aanbevolen acties.
Bewaar dit document voor uw administratie.

Veiligheids - Kwestie

Er zijn kwetsbaarheden voor cyberaanslagen geïdentificeerd wanneer bepaalde versies van de CARESCAPE Telemetrie-server, Apex Telemetrie-server, CARESCAPE Central Station (CSCS) versie 1 en Central Information Center (CIC) -systemen zijn verbonden met de Mission Critical (MC) en/of Information Exchange (IX) -netwerken.

De MC- en IX-netwerken zijn geïsoleerd van andere ziekenhuisnetwerken en -verkeer. Dit probleem kan zich daarom voordoen als de ongeautoriseerde persoon fysieke toegang heeft tot de bewakingsapparaten zelf of rechtstreeks toegang verkrijgt tot de geïsoleerde MC- of IC-netwerken ter plaatse in het ziekenhuis.

Als een ongeautoriseerd persoon met speciale vaardigheden dit niveau van toegang verkrijgt, kan de combinatie van een blootgegeven persoonlijke code, blootgegeven diensten en componenten met geïdentificeerde softwarekwetsbaarheden mogelijk misbruikt worden en gecombineerd met verdere gerichte schadelijke actie om:

- Wijzigingen aan te brengen aan het besturingssysteem van het apparaat waardoor o.a. het systeem onbruikbaar wordt, en/of
- Diensten te benutten die gebruikt worden voor externe weergave en controle van apparaten op het netwerk om toegang te verkrijgen tot de klinische gebruikersinterface en wijzigingen aan te brengen aan apparaatinstellingen en alarmgrenzen.

In deze situatie kunnen zulke cyberaanvallen mogelijk het wegvallen van de bewaking en/of uitblijven van alarmen tijdens actieve patiëntbewaking tot gevolg hebben.

Er is geen melding gemaakt van het optreden van incidenten door zo'n cyberaanval in een klinische gebruiksomgeving of letsels als gevolg van dit probleem.

Veiligheids - Instructies

U kunt uw product blijven gebruiken. Volg de Netwerkconfiguratiegids patiëntbewaking, CARESCAPE Netwerkconfiguratiegids en de Technische handleidingen en Onderhoudshandleidingen van uw product voor informatie over de juiste configuratie van de patiëntbewakingsnetwerken.

Naast het toepassen van de beste praktijken voor netwerkbeheer dient u er ook voor te zorgen dat:

1. MC- en IX-netwerken zijn geïsoleerd;
2. MC- en IX-routers/firewalls inkomend verkeer blokkeren, indien van toepassing;
3. Er beperkte fysieke toegang is tot Central Stations, Telemetrie-servers, het MC-netwerk en IX-netwerk;
4. Standaardwachtwoorden worden gewijzigd, indien van toepassing; en
5. Beste praktijken voor wachtwoordbeheer worden nageleefd.

Zorg ervoor dat de juiste configuratie en isolatie van de netwerken bescherming biedt tegen deze mogelijke problemen en het risico beperkt.

Details Betrokken Product

Als onderdeel van de voortdurende updates i.v.m. cyberbeveiligingszorg, ontwikkelt GE software-updates/patches waaronder beveiligingsverbeteringen. Klanten kunnen de beveiligingswebsite van GE bezoeken (https://securityupdate.gehealthcare.com) voor de meest recente informatie en zich aanmelden voor het ontvangen van kennisgevingen wanneer er nieuwe updates/patches beschikbaar zijn.

Bewaar deze kennisgeving bij uw handleidingen voor naslag in de toekomst.

Product-Correctie

Zie onderstaande tabel voor het identificeren van de betrokken producten. De identificatienummers zijn te vinden op het productlabel aan de achterkant van de eenheid. Het betrokken product is te herkennen aan het GE Healthcare-serienummer van 9, 10, 11 of 13 cijfers.

Productcodes per product:

Product	Productcode
Telemetrie-servers	GU, 3F, 4T, SAH, SEE
Central Stations	JA1, SCH, EF, 4T, AA1, GX, GQ, GU, SDY, SDZ, SGL, SGJ, SGK

Serienummer server: 13 cijfers	Serienummer server: 9, 10, of 11 cijfers
XXX XX XX XXXX XX Productidentificatiecode van drie cijfers	XX XX XXXX X XX Productidentificatiecode van twee cijfers

Contact-informatie

Indien u enige vragen heeft met betrekking tot deze correctieve actie of de identificatie van de betrokken items, neem dan contact op met uw lokale Sales/Service vertegenwoordiger.

GE Healthcare

De Wel 18

3871 MV Hoevelaken

033-2541250

GE Healthcare bevestigt dat dit bericht is gemeld aan de betreffende bevoegde instantie.

Wij verzekeren u dat het behoud van een hoog niveau van veiligheid en kwaliteit onze hoogste prioriteit heeft. Neem bij vragen alstublieft onmiddellijk contact met ons op.

Met vriendelijke groet,

xxx xxx

GE Healthcare

GEHC Ref nr. 36142

BEVESTIGING KENNISGEVING MEDISCH INSTRUMENT
ANTWOORD VEREIST

Vul dit formulier in en retourneer het zo spoedig mogelijk aan GE Healthcare, uiterlijk binnen 30 dagen na ontvangst. Hiermee wordt de ontvangst van en inzicht in de Kennisgeving inzake correctie van medische apparatuur Ref nr. 36142 bevestigd.

Naam klant/ontvanger: _____

Adres: _____

Stad/Provincie/Postcode/Land: _____

E-mailadres: _____

Telefoonnummer: _____

☐ Wij bevestigen ontvangst van en inzicht in de bijbehorende Kennisgeving inzake medische apparatuur en dat we het betrokken personeel hebben geïnformeerd en de gepaste maatregelen in overeenstemming met die Kennisgeving hebben genomen of zullen deze nemen.

Geef de naam van de persoon die verantwoordelijk is en dit formulier heeft ingevuld.

Handtekening: _____

Titel: _____

Datum (DD/MM/JJJJ): _____

Scan het ingevulde formulier of neem er een foto van en stuur dit/die per e-mail naar:
Recall.36142@ge.com

De onderstaande QR-code kan worden gebruikt om dit e-mailadres te verkrijgen: