PILNE ZAWIADOMIENIE DOTYCZĄCE BEZPIECZEŃSTWA

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

Znak wewn. GE Healthcare: FMI 36142

27 stycznia 2020

Do: Dyrektor ds. inżynierii biomedycznej / klinicznej
Dyrektorów ds. bezpieczeństwa IT
Administratorów ds. opieki zdrowotnej / kierowników ds. ryzyka

DOTYCZY: **Podatność na zagrożenia pewnych stacji centralnych GE i serwerów telemetrii ApexPro**

Ten dokument zawiera ważne informacje dotyczące zakupionego produktu. Prosimy upewnić się, że wszyscy użytkownicy w Państwa jednostce zapoznali się z treścią niniejszego powiadomienia dot. bezpieczeństwa wraz z zalecanymi działaniami. Ten dokument należy przechowywać w aktach.

Problem dotyczący bezpieczeństwa

Podczas podłączania do sieci Mission Critical (MC) i/lub Information Exchange (IX), w pewnych wersjach serwerów telemetrii CARESCAPE Telemetry Server, serwerów telemetrii Apex Telemetry Server, stacji centralnych CARESCAPE Central Station (CSCS) wersja 1 oraz systemów Central Information Center (CIC) znaleziono podatności na ataki cybernetyczne.

Sieci MC i IX są izolowane od pozostałych sieci szpitalnych. W związku z tym, aby problem wystąpił, nieupoważniona osoba musiałaby uzyskać fizyczny dostęp do urządzeń monitorujących lub do odizolowanych sieci MC lub IX znajdujących się w szpitalu.

Jeżeli nieupoważniona osoba, mająca odpowiednie umiejętności, uzyska taki poziom dostępu, kombinacja odkrytego klucza prywatnego, odkrytych usług oraz podzespołów o zidentyfikowanych podatnościach mogłaby zostać wykorzystana i połączona z dalszymi ukierunkowanymi złośliwymi działaniami:

- Wprowadzeniem zmian na poziomie systemu operacyjnego urządzenia, powodując, że urządzenie nie nadaje się do użytku i/lub
- Skorzystaniem z usług zdalnego podglądu i sterowania urządzeniami w sieci w celu uzyskania dostępu do interfejsu użytkownika klinicznego oraz wprowadzania zmian w ustawieniach urządzeń i ograniczeniach alarmowych.

W takiej sytuacji tego typu ataki cybernetyczne mogłyby potencjalnie skutkować w utracie możliwości monitorowania i/lub utracie alarmów podczas aktywnego monitorowania pacjentów.

Nie odnotowano żadnych przypadków ataku cybernetycznego w środowisku klinicznym lub jakichkolwiek zgłoszonych obrażeń w wyniku tej sprawy.

Instrukcje dotyczące bezpieczeństwa

Mogą Państwo nadal korzystać z opisywanego produktu. Aby zapoznać się z informacjami o prawidłowej konfiguracji sieci monitorów pacjentów, należy przestrzegać dokumentów Patient Monitoring Network Configuration Guide, CARESCAPE Network Configuration Guide oraz instrukcji technicznych i serwisowych produktu.

Poza stosowaniem dobrych praktyk zarządzania siecią, należy upewnić się, że:

1. sieci MC i IX są odizolowane;
2. router/zapora MC i IX blokuje ruch przychodzący, zgodnie z konfiguracją;
3. dostęp fizyczny do stacji centralnych, serwerów telemetrii, sieci MC oraz sieci IX jest ograniczony;
4. domyślne hasła są zmieniane zgodnie z harmonogramem; oraz
5. stosowane są dobre praktyki zarządzania hasłami

Upewnienie się, że sieci są prawidłowo skonfigurowane i odizolowane chroni przed tymi potencjalnymi obawami i ogranicza ryzyko.

Dane szczegółowe problematycznego produktu

W ramach aktualizacji zasad bezpieczeństwa cybernetycznego, firma GE rozwija aktualizacje/łatki, które zawierają usprawnienia bezpieczeństwa. Klienci mogą wejść na stronę bezpieczeństwa GE (https://securityupdate.gehealthcare.com) i otrzymać najnowsze informacje, jak również zapisać się do otrzymywania powiadomień, gdy dostępne są nowe aktualizacje/łatki.

Należy zachować tę informację z instrukcjami do wykorzystania w przyszłości.

Korekta dotycząca produktu

Należy zapoznać się z poniższą tabelą w celu identyfikacji dotkniętych produktów. Numery identyfikacyjne znajdują się na etykiecie produktu z tyłu urządzenia. Dotknięty produkt należy zidentyfikować, znajdując 9-, 10-, 11- lub 13- cyfrę numeru seryjnego GE Healthcare.

Kody produktu według produktu:

Produkt	Kod produktu
Serwery telemetrii	GU, 3F, 4T, SAH, SEE
Stacje centralne	JA1, SCH, EF, 4T, AA1, GX, GQ, GU, SDY, SDZ, SGL, SGJ, SGK

Numer seryjny serwera: 13 cyfr	Numer seryjny serwera: Cyfra 9, 10 lub 11
XXX XX XX XXXX XX Trzycyfrowy identyfikator produktu	XX XX XXXX X XX Dwucyfrowy identyfikator produktu

Informacje kontaktowe

W razie jakichkolwiek pytań związanych z powyższą "Informacją dotyczącą bezpieczeństwa produktu" bądź z określeniem zakresu objętych nią produktów, uprzejmie prosimy o kontakt z lokalnym przedstawicielem sprzedaży lub serwisu GE.

GE Healthcare potwierdza, iż niniejszy dokument został przekazany do wiadomości odpowiednich organów państwowych.

Pragniemy zapewnić, że utrzymanie wysokiego poziomu bezpieczeństwa stanowi dla nas najwyższy priorytet. W przypadku jakichkolwiek pytań, prosimy o natychmiastowy kontakt.

Dziękujemy!

Laila Gurney
Senior Executive, Global Regulatory and Quality
GE Healthcare

Jeff Hersh, PhD MD
Chief Medical Officer
GE Healthcare

GE Healthcare

GEHC nr ref. 36142

POTWIERDZENIE OTRZYMANIA INFORMACJI O URZĄDZENIU MEDYCZNYM
ODPOWIEDŹ JEST WYMAGANA

Należy wypełnić niniejszy formularz i odesłać go do firmy GE Healthcare niezwłocznie po otrzymaniu i nie później niż w ciągu 30 dni od jego otrzymania. Będzie to oznaczać potwierdzenie otrzymania i zapoznania się z Powiadomieniem o korekcie wyrobu medycznego nr ref. 36142.

Nazwisko/nazwa Klienta/Odbiorcy: _____

Adres: _____

Miasto/województwo/kod pocztowy/kraj: _____

Adres e-mail: _____

Numer telefonu: _____

☐ Potwierdzamy otrzymanie i przyjęcie do wiadomości informacji zawartych w załączonym Powiadomieniu o wyrobie medycznym, poinformowanie odpowiedniego personelu medycznego oraz podjęcie, obecnie i w przyszłości, odpowiednich działań zgodnie z treścią tego powiadomienia.

Należy podać imię i nazwisko osoby odpowiedzialnej za wypełnienie tego formularza.

Podpis: _____

Stanowisko: _____

Data (DD/MM/RRRR): _____

Prosimy zwrócić wypełniony formularz w postaci skanu lub zdjęcia, wysyłając go pod adres e-mail:
Recall.36142@ge.com

Ten adres e-mail można uzyskać za pomocą poniższego kodu QR: