Do wszystkich użytkowników systemów VD12A Sensis / Sensis Vibe

| | | | |
|---|---|---|---|
| Produkt/nazwa handlowa: | Sensis,<br>Sensis Vibe Combo,<br>Sensis Vibe Hemo | E-mail | piotr.adamczewski@siemens-healthineers.com |
| | | Data | Marzec 2021 r. |
| Numer modelu: | 10764561,<br>11007642,<br>11007641 | Id. działania korygującego | AX073/20/S |

# Informacja dla klientów dotycząca bezpieczeństwa w sprawie działania korygującego

**Temat: Problem z oprogramowaniem: „uprawnienia usług w systemie Windows”**

Szanowni Państwo!

W niniejszym piśmie informujemy o działaniu korygującym, które zostanie podjęte w celu skuteczniejszego zabezpieczenia Państwa systemu pod względem informatycznym.

## Na czym polega problem i kiedy występuje?

Z powodu konfiguracji niektórych „uprawnień usług w systemie Windows” na komputerze systemu Sensis Vibe istnieje ryzyko ujawnienia wrażliwych informacji, zmanipulowania danych lub ataku typu „odmowa usługi” (DoS). Atak może być podjęty z zewnątrz przy wykorzystaniu sieci IT szpitala i znanej nazwy użytkownika w systemie Windows systemu Sensis albo poprzez bezpośredni fizyczny dostęp do systemu.

## Jaki jest wpływ na działanie systemu i jakie są potencjalne zagrożenia?

W przypadku ataku cybernetycznego zmanipulowanie przez agresora wrażliwych danych dotyczących zabiegu może spowodować podjęcie nieprawidłowych decyzji diagnostycznych lub terapeutycznych.
Ataki typu „odmowa usługi” (DoS) mogą spowodować niedostępność systemu.

## W jaki sposób wykryto problem i jaka jest jego podstawowa przyczyna?

Problem został wykryty podczas regularnego wewnętrznego poszukiwania luk w zabezpieczeniach IT.

**Jakie działania musi podjąć użytkownik, aby uniknąć zagrożeń związanych z tym problemem?**

Nie istnieje obejście tego problemu. W każdym przypadku należy zapewnić możliwość kontynuowania leczenia pacjenta w inny sposób, jeśli istnieje jakiekolwiek potencjalne zagrożenie dla pacjenta.

**Jakie działania podejmuje producent w celu zminimalizowania ryzyka?**

„Uprawnienia usług w systemie Windows" zostaną ograniczone do minimalnego niezbędnego poziomu.

**Jaka jest skuteczność działania korygującego?**

Luka w zabezpieczeniach IT systemu zostanie zmniejszona.

**W jaki sposób działanie korygujące zostanie zrealizowane?**

Nasz serwis skontaktuje się z Państwem w celu umówienia się na termin przeprowadzenia powyższego działania korygującego.
Niniejsze pismo zostanie rozesłane do klientów, których dotyczy ten problem, jako aktualizacja AX074/20/S.

**Jakie jest ryzyko dla pacjentów, którzy byli wcześniej badani lub leczeni przy użyciu tego systemu?**

Producent nie dostrzega ryzyka dla pacjentów, którzy byli wcześniej badani lub leczeni.

Prosimy dopilnować, aby odpowiednie informacje dotyczące bezpieczeństwa przedstawione w niniejszym komunikacie otrzymali w Państwa organizacji wszyscy użytkownicy produktów, których one dotyczą, a także inne osoby, które powinny te informacje otrzymać.
Dziękujemy za zrozumienie i współpracę oraz prosimy o natychmiastowe przekazanie odpowiednich instrukcji dotyczących bezpieczeństwa personelowi. Niniejszy komunikat należy zachować w Państwa aktach dotyczących produktu. Informacje należy przechowywać przynajmniej do czasu ukończenia działań korygujących.
Prosimy także przekazać tę informację na temat bezpieczeństwa wszelkim innym organizacjom, dla których podejmowane czynności mogą być istotne.

Jeśli urządzenie, którego dotyczy komunikat, zostało sprzedane i zmienił się właściciel urządzenia, wówczas niniejszy komunikat należy przekazać nowemu właścicielowi. Prosimy również o przekazanie nam danych nowego właściciela, o ile jest to możliwe.

Wszelkie pytania dotyczące niniejszego komunikatu bezpieczeństwa prosimy kierować do lokalnego przedstawiciela firmy Siemens Healthcare, pod numer 0800 120 133

Z poważaniem

Piotr Adamczewski, Kierownik ds. Serwisu