Siemens Healthcare GmbH, HC AT IR MK, Siemensstr. 1, 91301 Forchheim

Do wszystkich użytkowników systemów Artis, X-Workplace, Sensis i Arcadis z przestarzałymi wersjami sprzętu lub oprogramowania

Imię i nazwisko dr Philip Stenner
Dział HC AT IR MK
E-mail philip.stenner@siemens-healthineers.com

Kontakt w Siemens Healthcare Sp. z o.o.

Imię i nazwisko Piotr Adamczewski
Dział HC CS
E-mail piotr.adamczewski@siemens-healthineers.com

Data 24 lipca 2017 r.

Ważna informacja dotycząca bezpieczeństwa: **AX047/17/S**

Informacja o luce w zabezpieczeniach systemu operacyjnego Microsoft Windows stosowanego w systemach Artis, X-Workplace, Sensis i Arcadis.

Szanowni Państwo!

Niniejsze pismo zawiera informacje o problemie z zabezpieczeniami informatycznymi, który potencjalnie może stwarzać zagrożenie dla pacjentów.

Na czym polega pierwotny problem i kiedy występuje?

W systemach Artis, X-Workplace, Sensis i Arcadis używane są systemy operacyjne Windows XP i Windows 7. Luka w zabezpieczeniach tych systemów operacyjnych jest źródłem poważnego zagrożenia.
Szkodliwe oprogramowanie, znane jako wirus „WannaCry", wykorzystuje tę lukę do ataków na narażone systemy i uszkadza przechowywane w nich dane, szyfrując je.

Więcej informacji technicznych można znaleźć w serwisie internetowym firmy Siemens:
http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-023589.pdf

Jaki jest wpływ problemu na działanie systemu i jakie jest potencjalne ryzyko?

Szkodliwe oprogramowanie szyfruje dane w zaatakowanych systemach. Zaszyfrowanie części danych w systemie Artis, X-Workplace, Sensis lub Arcadis może doprowadzić do sytuacji, w której konieczne będzie anulowanie leczenia, rozpoczęcie go od początku lub przeniesienie do działającego systemu. Skutkiem pośrednim może być również utrata uzyskanych wcześniej danych.

Jakie działania mogą podjąć użytkownicy?

Możliwość wykorzystania takiej luki w zabezpieczeniach zależy od konfiguracji produktu i środowiska, w jakim jest wdrożony. Firma Microsoft informuje, że wspomniane oprogramowanie wymuszające okup rozprzestrzenia się w załącznikach/łączach zawartych w wiadomościach e-mail typu phishing, a także w szkodliwych witrynach internetowych („infekcja systemu zerowego") lub przez zainfekowany system, który wykorzystuje lukę w zabezpieczeniach komponentu systemu Windows obsługującego udziały plikowe (udostępnione pliki) z systemów w tej samej sieci. Wybrane szczegółowe informacje można znaleźć na następującej stronie firmy Microsoft:
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacryptattacks/

Pragniemy podkreślić, że ani korzystanie z klienta poczty e-mail, ani przeglądanie stron internetowych nie mieści się w przeznaczeniu większości naszych produktów.

Zalecenia

Systemy, których dotyczy niniejsze pismo i które zostały wymienione w następnym akapicie, zawierają sprzęt lub oprogramowanie mające status przestarzałego.
W systemach tych nie można zainstalować poprawki firmy Microsoft.

Arcadis:

Arcadis Varic	(nr kat. 8080017)
Arcadis Orbic	(nr kat. 8081080)
Arcadis Avantic	(nr kat. 10048590)
Arcadis Varic Gen2	(nr kat. 10143406) o numerach seryjnych niższych od 15000
Arcadis Orbic Gen2	(nr kat. 10143407) o numerach seryjnych niższych od 23000
Arcadis Avantic Gen2	(nr kat. 10143408) o numerach seryjnych niższych od 33000

syngo X-WP:

X-Leonardo	VA70, VA71, VA72, VB11A/B, VB11M,

Powyższe produkty nasłuchują na portach sieciowych 139/tcp, 445/tcp lub 3389/tcp.
Poziom ich narażenia na wykorzystanie luki w zabezpieczeniach zależy od środków bezpieczeństwa stosowanych w sieci.
Aby zabezpieczyć narażony produkt, należy odseparować go od potencjalnie zainfekowanych systemów w tym samym segmencie sieci (np. produkt zainstalowany w segmencie sieci powinien być chroniony przez zaporę, która blokować będzie dostęp do portów sieciowych 139/tcp, 445/tcp i 3389/tcp).

Jeśli nie jest możliwe zaimplementowanie powyższego rozwiązania, zalecamy następujące działania:
Jeśli nie spowoduje to narażenia pacjentów na niebezpieczeństwo ani pogorszenia jakości leczenia, należy odłączyć niezainfekowany produkt od sieci i używać go w trybie autonomicznym.

W przypadku następujących systemów zalecamy aktualizację przestarzałego oprogramowania systemu do wersji aktualnej, w której będzie można zainstalować poprawkę firmy Microsoft:

Artis:

AXIOM Artis	VB22N, VB23D/F/G/H/J	➔ prosimy zaktualizować do VB23P
AXIOM Artis	VB30C/E, VB31E/F, VB35A	➔ prosimy zaktualizować do VB35E
Artis zee	VC13A/B, VC13D/E, VC14B/D/E/G	➔ prosimy zaktualizować do VC14J
Artis zee	VC21A	➔ prosimy zaktualizować do VC21C
Artis One	VA10B, VA10C	➔ prosimy zaktualizować do VA10D

syngo X-WP:

syngo X-WP	VB13E	➔ prosimy zaktualizować do VB13F
syngo X-WP	VB14A, VB14B	➔ prosimy zaktualizować do VB14C
syngo X-WP	VB15B, VB15C	➔ prosimy zaktualizować do VB15D
syngo X-WP	VB20B, VB20C	➔ prosimy zaktualizować do VB20D
syngo X-WP	VB21B	➔ prosimy zaktualizować do VB21C
syngo X-WP	VC10C	➔ prosimy zaktualizować do VC10D

Sensis:

Sensis	VC03A/B/C/D	➔ prosimy zaktualizować do VC03G lub nowszej wersji
Sensis	VC10B/C, VC11A/B/C	➔ prosimy zaktualizować do VC11D lub nowszej wersji
Sensis	VC12A	➔ prosimy zaktualizować do VC12C lub nowszej wersji
Sensis	VC12K	➔ prosimy zaktualizować do VC12L lub nowszej wersji

Ponadto firma Siemens Healthineers zaleca, co następuje:

Należy przygotować odpowiednie procedury odtwarzania kopii zapasowych i przywracania sprawności systemów.

W jaki sposób problem został wykryty?

Zagrożenie zostało wykryte w związku ze zgłoszeniami infekcji sprzętu prywatnego, przemysłowego i używanego w służbie zdrowia. Należy przyjąć, że analogiczna luka w zabezpieczeniach występuje w systemach Artis, X-Workplace, Sensis i Arcadis.

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

W tym przypadku nie uważamy, by konieczne było ponowne badanie pacjentów. Problem polega na możliwej usterce, która nie ma wpływu na leczenie pacjentów.

Z góry dziękujemy za Państwa współpracę w związku z sytuacją opisaną w niniejszym komunikacie i prosimy o niezwłoczne powiadomienie odpowiednich pracowników Państwa organizacji, którzy powinni otrzymać informacje o tym problemie. 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.

Z poważaniem,

Siemens Healthcare GmbH
Obszar biznesowy AT

Dr Heinrich Kolem	Wolfgang Hofmann
Prezes ds. terapii zaawansowanych (AT)	Pełnomocnik ds. bezpieczeństwa wyrobów medycznych