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

Data 19.06.2017

Do wszystkich użytkowników systemów Artis, X-Workplace, Sensis i Arcadis

–

Ważny komunikat dla klientów dotyczący bezpieczeństwa i działania korygującego, które zostanie podjęte w miejscu instalacji:

AX038/17/S, AX039/17/S, AX041/17/S, AX042/17/S, AX046/17/S, AX043/17/S

Informacja o działaniach korygujących dotyczących systemów Artis, X-Workplace, Sensis i Arcadis podejmowanych w celu wyeliminowania słabego punktu zabezpieczeń systemu operacyjnego Microsoft Windows.

Szanowni Państwo!

W niniejszym piśmie informujemy o działaniu korygującym, które zostanie podjęte w celu zapobieżenia potencjalnemu zagrożeniu dla pacjentów.

Na czym polega problem będący przyczyną podjęcia działania korygującego i kiedy problem ten występuje?

W systemach Artis, X-Workplace, Sensis i Arcadis używane są systemy operacyjne Windows XP i Windows 7. Słaby punkt zabezpieczeń tych systemów operacyjnych jest źródłem poważnego zagrożenia. Szkodliwe oprogramowanie, znane jako wirus „WannaCry”, wykorzystuje ten słaby punkt 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 działanie zostanie podjęte?

Oprogramowanie w narażonych systemach zostanie zaktualizowane w celu wyeliminowania słabego punktu zabezpieczeń w systemie operacyjnym Microsoft Windows. Przygotowano następujące poprawki do wprowadzenia w miejscu instalacji systemu:

AX038/17/S –	ARTIS:	OS HOTFIX-UPDATE WIN XP SMB VULNERABILITY
AX039/17/S –	ARTIS:	OS HOTFIX-UPDATE WIN 7 SMB VULNERABILITY
AX041/17/S –	X-WP:	OS HOTFIX UPDATE WIN XP SMB VULNERABILITY
AX042/17/S –	X-WP:	OS HOTFIX UPDATE WIN 7 SMB VULNERABILITY
AX046/17/S –	SENSIS:	OS HOTFIX UPDATE SMB VULNERABILITY
AX043/17/S -	ARCADIS:	OS HOTFIX-UPDATE WIN XP SMB

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 analogiczny słaby punkt zabezpieczeń występuje w systemach Artis, X-Workplace, Sensis i Arcadis. Do tej pory zgłoszono jeden niepowiązany z innymi przypadek infekcji systemu Sensis.

Na ile skuteczne są działania korygujące?

Aktualizacja oprogramowania wyeliminuje przyczynę, zapewniając ochronę przed atakami oprogramowania ransomware o nazwie „WannaCry" i innego szkodliwego oprogramowania wykorzystującego słabe punkty zabezpieczeń systemu MS Windows, które eliminuje poprawka.

W jaki sposób działanie korygujące zostanie zrealizowane?

Aktualizacja oprogramowania zostanie przeprowadzona zdalnie. Tam, gdzie nie będzie to możliwe, nasz serwis wkrótce skontaktuje się z Państwem w celu ustalenia terminu wykonania tego działania korygującego. Aby ustalić wcześniejszy termin, mogą Państwo sami skontaktować się z naszym serwisem. Niniejsze pismo zostanie rozesłane do klientów, których dotyczy ten problem, jako aktualizacja **AX037/17/S**.

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,

Piotr Adamczewski,
Kierownik ds. Serwisu