Siemens Healthcare GmbH, HC DI SY, Henkestr. 127, 91052 Erlangen

Imię i nazwisko Vincent Schets
Dział HC SV DS PLM PACS

Telefon +49 (9131) 84-8169

Nasz numer referencyjny SY029-17-S

Data 29 maja 2017 roku

– **INFORMACJA DLA KLIENTA**

Do wszystkich użytkowników produktów opisanych w punkcie SZCZEGÓŁOWE INFORMACJE O PRODUKCIE

Informacje dla Klienta dotyczące złośliwego oprogramowania WannaCry zagrażającego produktom Syngo oraz innym produktom firmy Siemens Healthineers do elektronicznych usług zdrowotnych

Drogi Kliencie,

Firma Siemens Healthineers zdaje sobie sprawę z tego, że Państwa organizacja może się zmagać ze skutkami poważnego cyberataku, który został niedawno przeprowadzony przy użyciu oprogramowania „WannaCry".

Na czym polega ten problem i kiedy ma miejsce?

Niektóre produkty firmy Siemens Healthineers mogą być narażone na cyberataki przeprowadzane przy użyciu złośliwego oprogramowania typu ransomware znanego jako WannaCry, które wykorzystuje lukę w zabezpieczeniach oprogramowania Microsoft. Możliwość wykorzystania takiej luki w zabezpieczeniach zależy od rzeczywistej konfiguracji oraz środowiska wdrożenia każdego produktu. Według firmy Microsoft jest to program typu ransomware, który rozprzestrzenia się poprzez załączniki/linki w mailach phishingowych lub na złośliwych stronach internetowych („zainfekowanie systemu zero") lub poprzez zainfekowany system, który wykorzystuje lukę w zabezpieczeniach składnika systemu Windows używanego w kontekście dzielenia się plikami z innymi systemami w ramach tej samej sieci.

Niektóre szczegółowe dane można znaleźć na następującej stronie Microsoft:

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Pragniemy zauważyć, że ani korzystanie z poczty elektronicznej na stacji klienckiej, ani przeglądanie Internetu nie jest częścią zamierzonego wykorzystania większości produktów, których dotyczy niniejsze pismo.

Jakie kroki może podjąć użytkownik, by uniknąć tego problemu?

Produkty bez nasłuchu na portach sieciowych 139/tcp, 445/tcp oraz 3389/tcp nie powinny być narażone na lukę w zabezpieczeniach, o ile produkt jest używany zgodnie z zamierzonym przeznaczeniem i standardową konfiguracją.

Firma Siemens Healthineers przekazuje listę produktów (patrz następny punkt), dla których klienci mogą pobrać łatkę zgodnie z biuletynem bezpieczeństwa firmy Microsoft (Microsoft Security Bulletin MS17-010) [https://technet.microsoft.com/en-us/library/security/ms17-010.aspx] i zaleca jej natychmiastowe zastosowanie. Ponadto firma Siemens Healthineers wydaje poradniki Siemens dotyczące bezpieczeństwa (Siemens Security Advisories) wybranych produktów, dla których wymagane są określone informacje o krokach zaradczych.

W przypadku narażonych produktów z nasłuchem na sieciowych portach 139/tcp, 445/tcp lub 3389/tcp, ich narażenie na wykorzystanie zależy od środków bezpieczeństwa zastosowanych w obrębie sieci. Aby chronić narażony produkt przed wykorzystaniem, należy go odizolować z zainfekowanego systemu w obrębie danego segmentu sieci (np. poprzez umieszczenie produktu w segmencie sieci oddzielonym zaporą firewall, która blokuje dostęp do sieciowych portów 139/tcp, 445/tcp oraz 3389/tcp).

Jeżeli wdrożenie wyżej wymienionych środków nie jest możliwe, zalecamy, co następuje:

- Jeżeli bezpieczeństwo i leczenie pacjentów nie jest zagrożone, należy odłączyć niezainfekowany produkt z sieci i używać go w trybie autonomicznym.
- Należy ponownie podłączyć produkt dopiero po zainstalowaniu udostępnionej łatki w systemie lub po podjęciu kroków zaradczych.

Oprócz tego firma Siemens Healthineers zaleca:

- Sporządzenie odpowiednich kopii zapasowych oraz wprowadzenie procedur przywracania sprawności systemu.
- Pobieranie i instalowanie najnowszych aktualizacji zabezpieczeń.
- Informacje oraz porady dotyczące określonych łatek i kroków zaradczych można uzyskać, kontaktując się z lokalnym inżynierem serwisowym firmy Siemens Healthineers, portalem lub naszym Regionalnym Centrum Wsparcia.

SZCZEGÓŁOWE INFORMACJE O PRODUKCIE

Poprawki zabezpieczeń firmy Microsoft mogą być instalowane w połączeniu z następującymi produktami firmy Siemens Healthineers oraz produktami dystrybuowanymi przez firmę Siemens Healthineers:

· *syngo*.via®: Wszystkie wersje
· *syngo*.via Frontier: Wszystkie wersje
· *syngo*.via ProtoNeo: Wszystkie wersje

- *syngo*.WebViewer: Wszystkie wersje
- *syngo*.Dynamics: Wszystkie wersje
- *syngo*.plaza®: Wszystkie wersje
- *syngo*® Imaging: Wszystkie wersje na serwerze OPM oraz syngo Studio Zaawansowane oprogramowanie
- *syngo*® Workflow MLR: Wszystkie wersje
- *syngo*® Workflow SLR: Wszystkie wersje
- teamplay®: Wszystkie wersje
- syngo Imaging XS: Wszystkie wersje na serwerach oraz raportujących stacjach klienckich
- MagicLink A: Wszystkie wersje
- SIENET MagicWeb Server: Wszystkie wersje do VA50B_0207
- MagicView 1000W: Wersja VF50A oraz nowsze
- ResolutionMD: Wszystkie wersje

Jeżeli niezbędne są dodatkowe środki, rozesłane zostaną uzupełniające informacje o konkretnych produktach.

Więcej informacji można znaleźć na stronie: ProductCERT Security Advisories.
http://www.siemens.com/cert/

Przepraszamy za wszelkie niedogodności wynikające z tej sytuacji i z góry dziękujemy za Państwa zrozumienie.

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

Z poważaniem

Dr Frank Engel-Murke
Kierownik DS PACS Define

Oliver Klinkow
VP Marketing i Sprzedaż