Komunikat dla klientów
CAN 003-2017

Do: Kierownika Oddziału Radiologii
Kierownika Oddziału Medycyny Nuklearnej/Obrazowania PET
Inspektora ds. zarządzania ryzykiem
Użytkowników systemów i stanowisk Siemens SPECT, SPECT.CT, PET i PET.CT

Temat: Luki w zabezpieczeniach oprogramowania Microsoft

Szanowni klienci firmy Siemens Healthineers!

Uzyskaliśmy informacje o lukach w zabezpieczeniach oprogramowania firmy Microsoft, które mogą mieć wpływ na Państwa system.
Niedawno firma Microsoft poinformowała o szeregu luk w zabezpieczeniach implementacji wersji 1.x protokołu Server Message Block (SMBv1).

Jakie jest potencjalne ryzyko?

Na podstawie naszej oceny przypadków wykorzystania luk w zabezpieczeniach przez szkodliwe oprogramowanie i ich potencjalnego wpływu na nasze produkty będziemy dostarczać poprawki do oprogramowania jako jeden ze środków lepszego zabezpieczenia protokołu SMBv1.
Wspomniane luki w zabezpieczeniach stwarzają możliwość zdalnego wykonania kodu na Państwa urządzeniu z rodziny Molecular Imaging. Znany jest już jeden szkodliwy program wykorzystujący te luki, występujący pod nazwą kodową „WannaCry". W wyniku działania tego programu może dojść do zainstalowania oprogramowania wymuszającego okup w zainfekowanym systemie komputerowym.

Dotychczas nie dotarły do nas żadne doniesienia o zdarzeniach niepożądanych w którymkolwiek systemie Molecular Imaging, które miałyby związek z powyższym problemem.

Siemens Medical Solutions USA, Inc.
2501 N. Barrington Rd.
Hoffman Estates, IL 60192, USA

W jaki sposób można ograniczyć ryzyko?

W poniższej tabeli wymieniono wyroby medyczne z rodziny Molecular Imaging, w których luka w zabezpieczeniach — jeśli nie zostanie wyeliminowana — może zostać wykorzystana przez szkodliwe oprogramowanie. W tabeli podano również minimalne numery wersji oprogramowania potrzebne do zainstalowania poprawki:

Produkt	Minimalny nr wersji, w której można zainstalować poprawkę
SPECT E.CAM	VA46A
SPECT Symbia E	VA60A*
SPECT Symbia S	VA60A*
SPECT Symbia T/T2/T6/T16	VA60A*
SPECT Symbia Intevo T/T2/T6/T16	VB10A
SPECT Symbia Intevo Bold	VB20A
SPECT Symbia Evo	VB10A
SPECT Symbai Evo Excel	VB10A
SPECT Symbia.net	VA10C*
Stanowiska SPECT MI (V, P, C)	VA60A
PET Biograph HiRez 6/16	6.6.x (VF70x)
PET Biograph TruePoint 6/16/40/64	6.0.6 (VF16A), 6.5.4 (VF64A)
PET Biograph mCT i mCT Flow	VG50x
PET Horizon	VJ10x
PET Advanced Workflow (kreatory)	Odpowiednio do wersji skanera (powyżej)

**Poprawki nie można zainstalować w urządzeniach z oprogramowaniem w wersji VA70. W urządzeniach tych należy uaktualnić oprogramowanie do wersji VB10. Po uaktualnieniu możliwe będzie zainstalowanie poprawki.*

Numer wersji oprogramowania systemu można odczytać z tego menu głównego. Wystarczy w systemie menu wybrać kolejno opcje **HELP | ABOUT "Nazwa produktu"** (POMOC | INFORMACJE O „Nazwa produktu"), gdzie „Nazwa produktu" jest nazwą Państwa produktu. W razie trudności z ustaleniem numeru wersji oprogramowania prosimy skontaktować się z serwisem Siemens Service pod numerem podanym w niniejszym piśmie.

Jeśli system spełnia wskazane w piśmie wymagania co do minimalnej wersji oprogramowania, można zainstalować poprawkę na dwa sposoby:

1. Jeśli Państwa system jest serwisowany przez firmę Siemens i podłączony do usługi Siemens Remote Services (SRS), to poprawka zostanie automatycznie przekazana w ramach zdalnej aktualizacji Remote Update Handling (RUH).

Jeśli Państwa system nie jest podłączony do usługi SRS, to firma Siemens skontaktuje się z Państwem, aby zainstalować poprawkę w systemie.

Jeśli system nie spełnia wymagań co do minimalnej wersji oprogramowania, można skorzystać z innych środków ograniczających ryzyko:

1. Można zastosować zaporę sprzętową, która zablokuje porty 139/tcp, 445/tcp lub 3389/tcp; lub
2. Można odłączyć system od sieci lokalnej.

Ze względu na charakter tych luk w zabezpieczeniach firmy Microsoft firma Siemens Healthineers zdecydowanie zaleca, aby w przypadku systemów Molecular Imaging, w których nie można zainstalować

poprawki z powodu zbyt niskiego numeru wersji, zastosować jeden z powyższych środków w celu zabezpieczenia systemu przed zainfekowaniem szkodliwym oprogramowaniem.

Niniejszy komunikat należy dołączyć do Instrukcji obsługi systemu i rozpowszechnić wśród wszystkich operatorów systemu. Jeśli system, którego dotyczy ten komunikat, nie znajduje się już w Państwa posiadaniu, prosimy o przekazanie niniejszego pisma nowemu właścicielowi oraz poinformowanie firmy Siemens o zmianie właściciela.

Zdarzenia niepożądane lub problemy z jakością występujące podczas eksploatacji tego produktu należy zgłaszać firmie Siemens, korzystając z danych kontaktowych dostępnych poniżej.

Wszelkie pytania dotyczące niniejszego komunikatu dotyczącego bezpieczeństwa prosimy kierować do lokalnego przedstawiciela firmy Siemens. Odpowiednie numery kontaktowe podano poniżej.

- Ameryka: 1-800-888-7436
- Europa, Bliski Wschód i Afryka: +49 9131 940 4000
- Azja i Australia: +86 (21) 3811 2121
- * Polska: 0800 120 133

Dodatkowe źródła informacji:

[1] Microsoft Security Bulletin MS17-010:
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
[2] Więcej informacji i wskazówek dotyczących opisanych tutaj luk w zabezpieczeniach można znaleźć w naszym serwisie internetowym Siemens ProductCERT
http://www.siemens.com/cert/en/cert-security-advisories.htm

Z poważaniem,

Matt Shah
Wiceprezes, RA/QA & EHS
Molecular Imaging
CAN003-2017