Kundenwarnhinweis
CAN 003-2017

An: Leiter Radiologie
Leiter Nuklearmedizin/PET-Bildgebung
Risikomanagementbeauftragter
Anwender von SPECT-, SPECT.CT-, PET-, PET.CT-Systemen und -Workplaces von Siemens

Betreff: Sicherheitsanfälligkeiten der Microsoft-Software

Sehr geehrte Siemens Healthineers-Kundin, sehr geehrter Siemens Healthineers-Kunde,

wir wurden darüber informiert, dass es bei der Microsoft-Software Sicherheitsanfälligkeiten gibt, die Auswirkungen auf Ihr System haben können.
Microsoft hat vor kurzem eine Reihe von Sicherheitsanfälligkeiten an seinem Server Message Block Version 1.x (SMBv1) festgestellt und veröffentlicht.

Was sind die potenziellen Risiken?

Basierend auf der von uns durchgeführten Beurteilung zur möglichen Nutzung dieser Schadsoftware durch Dritte und zu potenziellen Auswirkungen auf unsere Produkte werden wir als eine Option zur Behebung dieser SMBv1-Sicherheitsanfälligkeiten Patches zur Verfügung stellen.
Diese Sicherheitsanfälligkeiten könnten eine Remotecodeausführung auf Ihrem Molecular Imaging-Bildsystem ermöglichen. Ein Exploit dieser Sicherheitsanfälligkeiten, bekannt als "WannaCry", wurde bereits bestätigt. Durch diesen Exploit kann es auf infizierten Computersystemen zur Installation von Ransomware kommen.

Derzeit liegen uns keine Berichte von negativen Ereignissen im Zusammenhang mit dieser Sicherheitsanfälligkeit auf Molecular Imaging-Systemen vor.

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

Wie können die potenziellen Risiken minimiert werden?

In der folgenden Tabelle finden Sie eine Auflistung der Molecular Imaging-Bildsysteme, die von diesem Problem betroffen sein können, wenn die Sicherheitsanfälligkeiten nicht behoben werden. Die für den Erhalt eines Patches mindestens erforderlichen Softwareversionen sind ebenfalls aufgeführt.

Produkt	Mindestversion für Patch
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 Symbia Evo Excel	VB10A
SPECT Symbia.net	VA10C*
SPECT MI Workplaces (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 und mCT Flow	VG50x
PET Horizon	VJ10x
PET Erweiterter Workflow (Wizards)	Basierend auf der/den oben genannten Scannerversion(en)
C.CAM Imaging System	Alle Versionen

**Geräte mit der Softwareversion VA70 können kein Patch erhalten. Diese Geräte sollten auf die Version VB10 hochgerüstet werden. Nach dem Upgrade ist der Patch anwendbar.*

Die Softwareversion Ihres Systems finden Sie im Hauptmenü der Software. Rufen Sie **HELP | ABOUT "Your Product"** (Hilfe | Informationen zu "Ihrem Produkt") aus dem Menü auf, wobei "Your Product" für den Namen des entsprechenden Produktes steht. Sollten Sie Schwierigkeiten haben, die Softwareversion zu ermitteln, wenden Sie sich bitte an Ihren Siemens-Ansprechpartner vor Ort unter den in diesem Schreiben aufgeführten Telefonnummern.

Sofern Ihr System über die in diesem Schreiben angegebenen Mindestsoftwareversionen verfügt, gibt es zwei Optionen für den Erhalt des Softwarepatches:

1. Wenn Siemens Ihr Servicedienstleister ist und Sie über eine Anbindung an Siemens Remote Services (SRS) verfügen, erhalten Sie den Patch automatisch als Push über Remote Update Handling (RUH).

Wenn Sie nicht über eine SRS-Anbindung verfügen, wird Siemens Sie kontaktieren, um die Patch-Installation auf Ihrem System durchzuführen.

Falls Ihr System die in diesem Schreiben angegebenen Mindestsoftwareanforderungen nicht erfüllt, gibt es folgende Möglichkeiten zur Risikominimierung:

1. Einrichtung einer Hardware-Firewall, um die Ports 139/tcp, 445/tcp oder 3389/tcp zu blockieren oder
2. Trennung des Systems von Ihrem lokalen Netzwerk

Aufgrund dieser Anfälligkeiten der Microsoft-Software empfiehlt Siemens Healthineers dringend, eine der oben genannten Optionen zu wählen, falls Ihr Molecular Imaging-System den Patch aufgrund der Software-Mindestanforderung nicht erhalten kann, um eine Infizierung mit Schadsoftware zu verhindern.

Sorgen Sie bitte dafür, dass dieser Kundenwarnhinweis in der Gebrauchsanweisung Ihres Systems hinterlegt und an alle Bediener des Systems weitergegeben wird. Wenn sich dieses Gerät nicht mehr in Ihrem Besitz befindet, möchten wir Sie bitten, dieses Informationsschreiben an den neuen Besitzer des Gerätes weiterzuleiten und Siemens über den Eigentümerwechsel zu informieren.

Negative Ereignisse und Qualitätsprobleme im Zusammenhang mit der Verwendung Ihres Systems sollten Siemens über die unten angegebenen Kontaktdaten gemeldet werden.

Falls Sie Fragen zu diesem Hinweis haben, wenden Sie sich bitte unter den unten angegebenen Nummern an Ihren Siemens-Ansprechpartner vor Ort.

–

- Amerika: 1-800-888-7436
- Europa, Naher Osten und Afrika: +49 9131 940 4000
- Asien und Australien: +86 (21) 3811 2121

Weitere Quellen:

[1] Microsoft Security Bulletin MS17-010:
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
[2] Weitere Informationen zu Sicherheitshinweisen im Zusammenhang mit diesen Sicherheitsanfälligkeiten finden Sie auf unserer Siemens ProductCERT-Website
http://www.siemens.com/cert/en/cert-security-advisories.htm

Mit freundlichen Grüßen

Intern Siemens Medical Solutions USA, Inc.

2501 N. Barrington Rd.
Hoffman Estates, IL 60192, USA