SIEMENS
Healthineers

Name:
Abteilung:
E-Mail [redacted]

An alle Benutzer von Artis-, X-Workplace-, Sensis- und ARCADIS-Systemen mit nicht mehr unterstützter Hard- und/oder Software

Datum Juni 28, 2017

Wichtiger Sicherheitshinweis: **AX047/17/S**

Informationen zu einer möglichen Schwachstelle im Betriebssystem Microsoft Windows für Artis-, X-Workplace-, Sensis- und ARCADIS-Systeme.

Sehr geehrte Kundin, sehr geehrter Kunde,

mit diesem Schreiben möchten wir Sie auf ein potenziell sicherheitsrelevantes Problem hinweisen, das eine Gefährdung von Patienten zur Folge haben kann.

Worin besteht das zugrundeliegende Problem und wann tritt es auf?

Die Systeme Artis, X-Workplace, Sensis und ARCADIS arbeiten mit den Betriebssystemen Windows XP und Windows 7. Eine Schwachstelle in diesen Betriebssystemen ist Ursache für eine akute Gefährdung. Eine Schadsoftware, der sogenannte "WannaCry"-Virus, nutzt diese Schwachstelle, um in empfindliche Systeme einzudringen und Daten auf diesen Systemen durch Verschlüsselung zu beschädigen.

Detaillierte technische Informationen finden Sie auf den Internetseiten von Siemens:
http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-023589.pdf

Wie wirkt sich das Problem auf den Systembetrieb aus und welches potenzielle Risiko besteht?

Die Schadsoftware verschlüsselt Daten auf dem befallenen System. Wenn Teile des Artis-, X-Workplace-, Sensis- oder ARCADIS-Systems verschlüsselt werden, kann es dazu kommen, dass die klinische Behandlung abgebrochen oder neu begonnen oder dass auf ein funktionierendes System gewechselt werden muss.
Eine indirekte Auswirkung kann außerdem sein, dass bereits erfasste Daten verloren gehen.

Welche Maßnahmen können Sie ergreifen?

Ob eine mögliche Sicherheitsanfälligkeit wirksam wird, hängt von der vorliegenden Konfiguration und Einsatzumgebung eines jeden Produkts ab. Laut Microsoft verbreitet sich die Ransomware entweder über Anhang/Link in Phishing-Mails, auf schadhaften Webseiten („Erstsysteminfektion") oder über ein infiziertes System, das eine Schwachstelle in einer Windows-Komponente ausnutzt, die im Zusammenhang mit offenen Dateifreigaben anderer Systeme genutzt wird, die über dasselbe Netzwerk zugänglich sind. Weitere Informationen finden Sie auf der folgenden Microsoft-Seite:
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacryptattacks/

Wir möchten darauf hinweisen, dass weder die Nutzung eines E-Mail-Clients noch das Surfen im Internet zum bestimmungsgemäßen Gebrauch der meisten in diesem Schreiben beschriebenen Produkte gehören.

Empfehlungen

Die Hard- und/oder Software der in diesem Schreiben genannten und im folgenden Abschnitt näher beschriebenen Systeme wird nicht mehr unterstützt.
Für folgende Systeme wird kein Microsoft Patch zur Verfügung gestellt:

Arcadis:

Arcadis Varic	(Sachnr. 8080017)
Arcadis Orbic	(Sachnr. 8081080)
Arcadis Avantic	(Sachnr. 10048590)
Arcadis Varic Gen2	(Sachnr.10143406) vor Seriennr. 15000
Arcadis Orbic Gen2	(Sachnr. 10143407) vor Seriennr. 23000
Arcadis Avantic Gen2	(Sachnr. 10143408) vor Seriennr. 33000

syngo X-WP:

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

Die oben genannten Produkte überwachen die Netzwerk-Ports 139/tcp, 445/tcp oder 3389/tcp.
Ihre Anfälligkeit ist abhängig von den Sicherheitsmaßnahmen im Netzwerk.
Um diese Produkte vor der Gefahr zu schützen, sollte es von allen infizierten Systemen im jeweiligen Netzwerkabschnitt isoliert werden (z. B. Produkte, die in einem Netzwerksegment eingesetzt werden, bei dem der Zugriff auf die Netzwerk-Ports 139/tcp, 445/tcp und 3389/tcp durch eine Firewall blockiert ist).

Wenn dies nicht umgesetzt werden kann, greifen folgende Empfehlungen:
Wenn kein Risiko für die Patientensicherheit und die Behandlung besteht, trennen Sie das nicht infizierte Produkt vom Netzwerk und nutzen Sie es im Standalone-Modus.

SIEMENS Healthineers

Für folgende Systeme empfehlen wir Ihnen dringend die Aktualisierung der nicht mehr unterstützten System-Software auf eine aktuelle Version, für die ein Microsoft Patch zur Verfügung gestellt wird:

Artis:

AXIOM Artis	VB22N, VB23D/F/G/H/J	→ bitte aktualisieren Sie auf VB23P
AXIOM Artis	VB30C/E, VB31E/F, VB35A	→ bitte aktualisieren Sie auf VB35E
Artis zee	VC13A/B, VC13D/E, VC14B/D/E/G	→ bitte aktualisieren Sie auf VC14J
Artis zee	VC21A	→ bitte aktualisieren Sie auf VC21C
Artis One	VA10B, VA10C	→ bitte aktualisieren Sie auf VA10D

syngo X-WP:

syngo X-WP	VB13E	→ bitte aktualisieren Sie auf VB13F
syngo X-WP	VB14A, VB14B	→ bitte aktualisieren Sie auf VB14C
syngo X-WP	VB15B, VB15C	→ bitte aktualisieren Sie auf VB15D
syngo X-WP	VB20B, VB20C	→ bitte aktualisieren Sie auf VB20D
syngo X-WP	VB21B	→ bitte aktualisieren Sie auf VB21C
syngo X-WP	VC10C	→ bitte aktualisieren Sie auf VC10D

Sensis:

Sensis	VC03A/B/C/D	→ bitte aktualisieren Sie auf VC03G oder eine spätere Version
Sensis	VC10B/C, VC11A/B/C	→ bitte aktualisieren Sie auf VC11D oder eine spätere Version
Sensis	VC12A	→ bitte aktualisieren Sie auf VC12C oder eine spätere Version
Sensis	VC12K	→ bitte aktualisieren Sie auf VC12L oder eine spätere Version

Außerdem empfiehlt Siemens Healthineers:
Stellen Sie sicher, dass Sie über die entsprechenden Sicherungen und Abläufe zur Systemwiederherstellung verfügen.

Wie wurde dieses Problem festgestellt?

Die Gefährdung wurde erkannt, nachdem der Befall entsprechender Ausrüstung im privaten, industriellen und Gesundheitsbereich bekannt wurde. Von einer Angreifbarkeit der Artis-, X-Workplace-, Sensis- und ARCADIS-Systeme muss ausgegangen werden.

Welche Risiken bestehen für Patienten, die zuvor mit diesem System untersucht/behandelt wurden?

Eine Nachuntersuchung des Patienten halten wir in diesem Fall nicht für notwendig. Es handelt sich hier um eine mögliche Störung, die keinen Einfluss auf die Patientenbehandlung hatte.

Wir danken Ihnen für Ihre Kooperation im Umgang mit diesem Sicherheitshinweis und bitten Sie, diese Informationen unverzüglich an alle Mitarbeiter in Ihrer Einrichtung weiterzugeben, die von diesem Problem wissen müssen, und diese entsprechend einzuweisen. Bitte leiten Sie diesen Sicherheitshinweis auch an andere Einrichtungen weiter, die ebenfalls von dieser Maßnahme betroffen sein könnten.

Falls das Gerät verkauft wurde und es daher nicht mehr in Ihrem Besitz ist, möchten wir Sie bitten, diesen Sicherheitshinweis an den aktuellen Besitzer weiterzuleiten. Wenn möglich, informieren Sie uns bitte über die Identität des aktuellen Besitzers.

Mit freundlichen Grüßen

Siemens Healthcare GmbH
AT Business Area

[redacted]

[redacted]