Siemens Healthcare S.r.l., V.le Piero e Alberto Pirelli, 10 - 20126 Milano

Al Responsabile della Unità Operativa presso cui è operativo il prodotto SIEMENS ed al responsabile amministrativo dell'Azienda Ospedaliera

Modality Manager Fulvio Fazion
Reparto HC Customer Services

Telefono 800.827.119
Fax 02.2436.3431
e-mail fulvio.fazion@siemens-healthineers.com
Data 18.07.2017

Avviso di sicurezza

A tutti gli utilizzatori dei sistemi Artis, di X-Workplace,
di sistemi Sensis e Arcadis con hardware o software obsoleto

Oggetto: vulnerabilità potenziale nel sistema operativo Microsoft Windows dei sistemi Artis, X-Workplace, Sensis e Arcadis.

Gentile Cliente,

Questa lettera per informarla di un potenziale problema rilevante per la sicurezza con eventuale rischio per i pazienti.

Qual è la situazione e quando accade

I sistemi Artis, X-Workplace, Sensis e Arcadis utilizzano i sistemi operativi Windows XP e Windows 7. Una vulnerabilità di questi sistemi operativi è la base di un pericolo incombente.
Un software maligno, conosciuto come virus "WannaCry", sfrutta questa vulnerabilità per invadere sistemi suscettibili e corrompere dati su questi sistemi tramite criptaggio.

Ulteriori informazioni tecniche sono disponibili al sito Internet Siemens:
http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-023589.pdf

Qual è l'impatto sul funzionamento del sistema e qual è il rischio potenziale?

Il software maligno cripta dati sui sistemi colpiti. Se parti del sistema Artis, di X-Workplace, del sistema Sensis o Arcadis sono state criptate, si potrebbe determinare una situazione in cui è necessario annullare o riavviare il trattamento clinico di un paziente o trasferirlo a un sistema funzionante.
Un effetto indiretto di ciò, è anche la possibilità di perdere dati acquisiti in precedenza.

SIEMENS Healthineers

Quali azioni si possono svolgere?

La possibilità di sfruttare una tale vulnerabilità dipende dalla attuale configurazione e dall'ambiente di installazione di ciascun prodotto. Secondo Microsoft questo software maligno (ransomware) si diffonde tramite allegati/link in email di phishing, o su siti Web maligni ("infezione zero del sistema"), oppure tramite un sistema infettato, che sfrutta una vulnerabilità in un componente Windows, utilizzato nel contesto delle condivisioni di file aperti di altri sistemi raggiungibili sulla stessa rete. Alcuni dettagli si possono trovare alla seguente pagina Microsoft:
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacryptattacks/
Vorremmo evidenziare che l'utilizzo di un client di email e la navigazione su Internet non rientrano nell'utilizzo previsto della gran parte dei nostri tipi di prodotto.

Raccomandazioni

I sistemi interessati da questa lettera e dettagliati nel seguente paragrafo hanno uno stato hardware o software obsoleto.
Per i seguenti sistemi, non è possibile utilizzare alcuna patch Microsoft.

Arcadis:

Arcadis Varic	(P/N 8080017)
Arcadis Orbic	(P/N 8081080)
Arcadis Avantic	(P/N 10048590)
Arcadis Varic Gen2	(P/N 10143406) precedente S/N 15000
Arcadis Orbic Gen2	(P/N 10143407) precedente S/N 23000
Arcadis Avantic Gen2	(P/N 10143408) precedente S/N 33000

syngo X-WP:

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

I prodotti di cui sopra si connettono alle porte 139/tcp, 445/tcp o 3389/tcp.
La loro esposizione alla diffusione del virus dipende dalle misure di sicurezza nella rete.
Per proteggere un sistema vulnerabile all'infezione, il prodotto dovrebbe essere isolato da qualsiasi sistema potenzialmente infetto nel proprio segmento di rete (per esempio, un prodotto utilizzato in un segmento di rete separato tramite controllo firewall con blocco dell'accesso alle porte di rete 139/tcp, 445/tcp ed 3389/tcp).

Se quanto sopra descritto non può essere implementato, si raccomanda di procedere come descritto di seguito:
Se la sicurezza e il trattamento del paziente non sono a rischio, disconnettere il prodotto non infettato dalla rete e utilizzarlo in modalità standalone.

Per i seguenti sistemi, si raccomanda di aggiornare il software di sistema obsoleto a una versione aggiornata per la quale è possibile utilizzare una patch Microsoft:

Artis:

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

syngo X-WP:

syngo X-WP	VB13E → aggiornare a VB13F
syngo X-WP	VB14A, VB14B → aggiornare a VB14C
syngo X-WP	VB15B, VB15C → aggiornare a VB15D
syngo X-WP	VB20B, VB20C → aggiornare a VB20D
syngo X-WP	VB21B → aggiornare a VB21C
syngo X-WP	VC10C → aggiornare a VC10D

Sensis:

Sensis	VC03A/B/C/D → aggiornare a VC03G o versione successiva
Sensis	VC10B/C, VC11A/B/C → aggiornare a VC11D o versione successiva
Sensis	VC12A → aggiornare a VC12C o versione successiva
Sensis	VC12K → aggiornare a VC12L o versione successiva

Inoltre, Siemens Healthineers raccomanda:
Assicurarsi di disporre degli appropriati backup e delle procedure di ripristino del sistema.

Come è stata rilevata la situazione?

La minaccia è stata identificata quando è stata indicata l'infezione di una determinata apparecchiatura privata, industriale e di healthcare. Si è dedotta una corrispondente vulnerabilità dei sistemi Artis, X-Workplace, Sensis e Arcadis.

Quali rischi vi sono per pazienti esaminati o trattati in precedenza con questo sistema?

In questo caso valutiamo che non è necessario riesaminare pazienti. Questo è un eventuale difetto che non ha alcuna influenza sul trattamento di pazienti.

Ringraziandovi per la collaborazione nell'acquisizione di questo avviso di sicurezza, vi chiediamo di informare e di istruire tempestivamente il personale della Vostra organizzazione che deve essere a conoscenza di questa situazione. Siete pregati inoltre di fornire queste informazioni di sicurezza anche ad altre organizzazioni che potrebbero essere interessate da questa azione.

Nel caso in cui questo dispositivo/apparecchio sia stato venduto e quindi non sia più in Suo possesso, La preghiamo di trasmettere il presente avviso di sicurezza al nuovo proprietario. Inoltre, La preghiamo di segnalarci il nuovo proprietario del dispositivo/apparecchio.

La sicurezza del paziente riveste per noi carattere prioritario. Confidiamo che questa comunicazione sia intesa come una scrupolosa attenzione che la nostra azienda pone, non solo nelle procedure di produzione, ma anche al costante monitoraggio della qualità dei prodotti presso gli utilizzatori al fine di assicurare il più elevato standard di qualità e sicurezza.

Vi preghiamo inoltre di voler conservare una copia di questa comunicazione nel vostro archivio e di volerla inoltrare a chiunque possa avere in uso il dispositivo oggetto del presente avviso di sicurezza.

Le chiediamo di voler cortesemente compilare e rispedire via fax il modulo di "conferma di avvenuta notifica" allegato al presente avviso di sicurezza al seguente numero:

Fax: 02.2436.3431 att.ne: Customer Care Center - Updates

Ci scusiamo per ogni inconveniente e per eventuali chiarimenti La invitiamo a contattare il nostro Customer Services al numero 800.827.119

Nel ringraziarLa per la collaborazione Le inviamo i nostri più distinti saluti.

Siemens Helathcare S.r.l.

G. Damonti

G. Ratti

Siemens Healthcare S.r.l

Società a Unico Socio soggetta alla Direzione e Coordinamento di Siemens AG

Viale Piero e Alberto Pirelli, 10
20126 Milano - Italia

Tel.: +39 02 243 1
Fax: +39 02 243 63696

www.siemens.it

SIEMENS Healthineers

Conferma di avvenuta notifica

Vi preghiamo di voler completare il presente Modulo e di inviarlo via fax al numero 02.2436.3431 att.ne: Customer Care Center - Updates

Indirizzo del cliente:

_____

_____

_____

Con la presente intendo confermare, in qualità di proprietario / operatore responsabile del prodotto denominato _____ recante il numero di serie _____(facoltativo), di avere ricevuto la documentazione di seguito indicata:

Avviso di sicurezza

Rif. AX047/17/S

Oggetto: vulnerabilità potenziale nel sistema operativo Microsoft Windows dei sistemi Artis, X-Workplace, Sensis e Arcadis.

Luogo, Data _____

Nome _____

Timbro e Firma _____

Siemens Healthcare S.r.l

Società a Unico Socio soggetta alla Direzione e Coordinamento di Siemens AG

Viale Piero e Alberto Pirelli, 10
20126 Milano - Italia

Tel.: +39 02 243 1
Fax: +39 02 243 63696

www.siemens.it