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 Germano Pizzorno
Reparto HC Customer Services

Telefono 800.827.119
Fax 02.2436.3431
e-mail germano.pizzorno@siemens.com
Data 14.06.2017

Avviso di sicurezza

A tutti gli utilizzatori dei sistemi descritti in
INFORMAZIONI SPECIFICHE SUI PRODOTTI

Oggetto: Informazioni per i clienti relative al malware WannaCry e ai prodotti Siemens Healthineers Syngo e Digital Health Services

Gentile Cliente,

Siemens Healthineers è consapevole del fatto che la Sua organizzazione potrebbe dover affrontare gli effetti del recente cyber-attacco noto come "WannaCry".

Qual è il problema e quando si presenta?

Alcuni prodotti Siemens Healthineers potrebbero essere stati colpiti a causa della vulnerabilità di Microsoft sfruttata dal ransomware WannaCry. L'esposizione a questo tipo di vulnerabilità dipende dalla configurazione corrente e dall'ambiente di implementazione di ciascun prodotto. Secondo quanto affermato da Microsoft, questo ransomware si diffonde tramite allegati/link in emali di phishing o in siti web dannosi ("system zero infection") oppure tramite un sistema infetto che sfrutta una vulnerabilità di un componente Windows utilizzato nel contesto di condivisioni aperte di file di altri sistemi raggiungibili nella stessa rete.

Per ulteriori informazioni, visitare la pagina Microsoft:
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Desideriamo far presente che l'uso di un client email o la navigazione in Internet non rientrano nell'uso previsto della maggior parte dei prodotti interessati dalla presente lettera.

Quali provvedimenti può adottare l'utilizzatore per evitare questo problema?

I prodotti che non sono in ascolto sulle porte di rete 139/tcp, 445/tcp e 3389/tcp non dovrebbero essere esposti alla vulnerabilità purché il prodotto venga utilizzato come previsto e nella configurazione standard.

Siemens Healthineers fornisce un elenco di prodotti (vedere la prossima sezione) che possono essere aggiornati con una patch da parte dei clienti come previsto dal Microsoft Security Bulletin MS17-010 [https://technet.microsoft.com/enus/librarv/security/ms17-010.aspx] e raccomanda che la patch venga installata immediatamente. Inoltre, Siemens Healthineers pubblica degli Avvisi per la sicurezza Siemens relativi ad alcuni prodotti che richiedono informazioni specifiche per la risoluzione del problema.

Per i prodotti vulnerabili in ascolto sulle porte di rete 139/tcp, 445/tcp o 3389/tcp, la loro esposizione alla violazione dipende dalle misure di sicurezza implementate nella rete. Per proteggere un prodotto vulnerabile da tale esposizione, si consiglia di isolarlo da qualsiasi sistema infetto all'interno del relativo segmento di rete (per esempio, prodotto implementato in un segmento di rete, separato mediante firewall che blocca l'accesso alle porte di rete 139/tcp, 445/tcp e 3389/tcp).

Se non è possibile implementare quanto sopra, raccomandiamo di fare quanto segue:

- Se la sicurezza e il trattamento dei pazienti non sono a rischio, scollegare il prodotto non infettato dalla rete e utilizzarlo in modalità standalone.
- Ricollegare il prodotto solo dopo aver installato la patch o il rimedio fornito sul sistema.

Siemens Healthineers raccomanda inoltre di fare quanto segue:

- Assicurasi di avere eseguito i backup e le procedure di ripristino del sistema appropriate.
- Assicurasi di installare gli aggiornamenti più recenti relativi alla sicurezza.
- Per informazioni di guida su patch o rimedi specifici, contattare il tecnico dell'assistenza clienti locale di Siemens Healthineers, il portale o il nostro centro di supporto regionale.

INFORMAZIONI SPECIFICHE SUI PRODOTTI

La patch MS17-010 per la sicurezza di Microsoft può essere installata con i seguenti prodotti Siemens Healthineers e i prodotti distribuiti da Siemens Healthineers:

- syngo.via®: tutte le versioni
- syngo.via Frontier: tutte le versioni
- syngo.via ProtoNeo: tutte le versioni
- syngo.WebViewer: tutte le versioni
- syngo.Dynamics: tutte le versioni
- syngo.plaza®: tutte le versioni
- syngrilD Imaging: tutte le versioni su server OPM e syngo Studio Advanced
- syngrilD Workflow MLR: tutte le versioni
- syngo® Workflow SLR: tutte le versioni
- ·teamplay®: tutte le versioni
- syngo Imaging XS: tutte le versioni su server e client di reporting
- Magiclink A: tutte le versioni
- SIENET MagicWeb Server: tutte le versioni fino alla VA50B_0207
- MagicView 1000W: versione VF50A e successive
- ResolutionMD: tutte le versioni

Nel caso in cui siano necessarie misure addizionali, verranno inviate informazioni aggiuntive sugli specifici prodotti.

Per ulteriori informazioni, visitare il nostro sito ProductCERT Security Advisories. http://www.siemens.corn/cert/.

Ci scusiamo per i disturbi che questa situazione le potrebbe causare e la ringraziamo in anticipo per la comprensione.

Siemens Healthcare S.r.l

Viale Piero e Alberto Pirelli, 10
20126 Milano - Italia

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

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

www.siemens.it

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 Healthcare 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. SY029/17/S

Oggetto: Informazioni per i clienti relative al malware WannaCry e ai prodotti Siemens Healthineers Syngo e Digital Health Services

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