



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 Mario Mauri  
Reparto HC Customer Services

Telefono 800.827.119  
Fax 02.2436.3431  
e-mail mario.mauri@siemens-healthineers.com  
Data 24.07.2017

### **Avviso di sicurezza**

- A tutti gli utilizzatori dei sistemi e workplace SPECT, SPECT.CT, PET, PET.CT Siemens

### **Oggetto: Vulnerabilità software Microsoft**

Gentile Cliente,

Siamo venuti a conoscenza di una vulnerabilità del software Microsoft che potrebbero influenzare il suo sistema.

Di recente, Microsoft ha reso nota una serie di vulnerabilità nell'implementazione del loro Server Message Block versione 1.x (SMBv1).

#### **Quali sono i rischi potenziali?**

Sulla base della nostra valutazione degli sfruttamenti malware e del potenziale impatto su nostri prodotti, offriremo come opzione una patch per risolvere la vulnerabilità SMBv1.

Queste vulnerabilità potrebbero consentire l'esecuzione di codice remoto sul dispositivo medicale di Imaging Molecolare. Lo sfruttamento di queste vulnerabilità è già emerso e il suo nome in codice è "WannaCry." Questo sfruttamento potrebbe consentire l'installazione di ransomware su sistemi di computer infettati.

Al momento, non abbiamo indicazioni di eventi avversi correlati a questa situazione su un sistema di Imaging Molecolare.

#### **Quali sono le possibili attenuazioni?**

La tabella che segue elenca i dispositivi di Imaging Molecolare che potrebbero essere sfruttati se le vulnerabilità non vengono contenute. La tabella indica anche la versione software minima richiesta per ricevere una patch:

Prodotto	Versione minima richiesta per ricevere il 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 Symbai Evo Excel	VB10A
SPECT Symbia.net	VA10C*
Workplace 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 ed mCT Flow	VG50x
PET Horizon	VJ10x
PET Advanced Workflow (Wizard)	Basato su versione(i) scanner di cui sopra

\*I dispositivi con versione software VA70 non sono adatti a ricevere una patch. Questi dispositivi dovrebbero essere invece aggiornati alla versione VB10. Una volta aggiornati, la patch potrà essere applicata.

L'indicazione della versione software del sistema si può trovare nel menu principale del software. Selezionare semplicemente **HELP | ABOUT "Your Product"** (Guida | Riguardo "il prodotto") dove "il prodotto" è il nome del prodotto in questione. In caso di difficoltà nella individuazione della versione software, contattare l'Assistenza Tecnica Siemens ai numeri telefonici forniti in questa lettera.

Se il sistema è dotato almeno della versione software minima indicata in questa lettera, vi sono due modi per ottenere la patch software:

1. Se Siemens offre la propria assistenza tecnica e si è connessi ai Siemens Remote Services (Servizi remoti Siemens) (SRS), la patch è immediatamente disponibile tramite la Remote Update Handling (Gestione aggiornamenti remota) (RUH).

Se non si è connessi agli SRS, si verrà contattati da Siemens per installare la patch sul sistema.

Se il sistema non è dotato almeno della versione software minima indicata in questa lettera, sono previste altre attenuazioni:

1. Si può utilizzare un firewall hardware per bloccare le porte 139/tcp, 445/tcp o 3389/tcp, oppure
2. Si può disconnettere il sistema dalla rete locale

A causa della natura di queste vulnerabilità del software Microsoft, se il sistema non è dotato almeno della versione software minima per ricevere una patch, Siemens Healthineers raccomanda vivamente di selezionare una delle opzioni di cui sopra per evitare che il sistema di Imaging Molecolare venga infettato con malware.

Assicurarsi che questo Avviso di sicurezza per il Cliente venga inserito nelle Istruzioni d'uso del sistema e che queste informazioni vengano distribuite a tutti gli operatori del sistema. Se questa apparecchiatura non è

Error! Reference source not found.

più in vostro possesso, vi chiediamo gentilmente di inoltrare questa lettera al nuovo proprietario dell'apparecchiatura, e di informare Siemens del cambio di proprietà.

Eventi avversi o problemi di qualità incontrati nell'utilizzo di questo prodotto devono essere notificati a Siemens tramite le informazioni di contatto di seguito indicate.

In caso di domande riguardanti questo avviso di sicurezza, contattare Siemens ai numeri telefonici indicati di seguito.

- America: 1-800-888-7436
- Europa, Medio Oriente e Africa: +49 9131 940 4000
- Asia e Australia: +86 (21) 3811 2121

— **Risorse aggiuntive:**

[1] Microsoft Security Bulletin MS17-010:

<https://technet.microsoft.com/en-us/library/security/ms17-010.aspx>

[2] Per ulteriori informazioni sugli avvisi di sicurezza associati a queste vulnerabilità, visitare il nostro sito Web Siemens ProductCERT

<http://www.siemens.com/cert/en/cert-security-advisories.htm>

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.

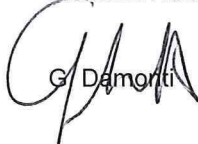
Le chiediamo di voler cortesemente compilare e rispedire via fax il modulo di "conferma di avvenuta notifica" allegato al presente avviso di sicurezza al seguente numero:

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.

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](http://www.siemens.it)

## 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. MI510/17/S

**Oggetto: Vulnerabilità software Microsoft**

Luogo, Data \_\_\_\_\_

Nome \_\_\_\_\_

Timbro e Firma \_\_\_\_\_