PHILIPS

****** AVVISO URGENTE PER LA SICUREZZA IN SITU ******

Oggetto: **sistemi Philips Volcano s5i, CORE, e CORE Mobile con versione software v3.5**

Novembre 21, 2017

Egregio Direttore del Laboratorio di Emodinamica:

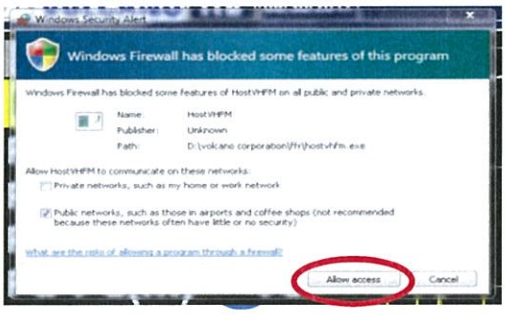
Philips Volcano sta avviando una correzione volontaria per risolvere un problema di configurazione che compromette alcuni sistemi s5i, CORE e CORE Mobile con versione software v3.5 ("Sistemi Compromessi"). Su alcuni Sistemi Compromessi, durante l'utilizzo potrebbe essere visualizzata una finestra di dialogo di sicurezza di Microsoft Windows inattesa e la risposta dell'utente alla finestra di dialogo potrebbe incidere negativamente sull'operazione successiva del dispositivo.

Se il vostro dispositivo soddisfa i criteri sottostanti, il vostro sistema potrebbe essere interessato:

Numero di identificazione del Prodotto	**Descrizione del Prodotto**	**Data di fabbricazione e versione del Software**
807400001	Volcano Imaging System s5i	23 marzo 2016 – 18 ottobre 2017 versione software v 3.5
400-0100.01, 400-0100.01-R 400-0100.07 400-0100.07-R 400-0100.08 400-0100.08-R	CORE Mobile Imaging System (120V) CORE Mobile Imaging System Refurbished CORE Mobile Imaging System (240V) CORE Mobile Imaging System Refurbished CORE Mobile Imaging System (100V) CORE Mobile Imaging System Refurbished	
400-0100.02	CORE Imaging System	

State ricevendo questa lettera perché i nostri registri indicano che potreste essere in possesso di un Sistema Compromesso.

Le impostazioni di sicurezza di Microsoft Windows su un esiguo numero di Sistemi Compromessi sono state configurate in modo erroneo durante il processo di fabbricazione. Questo errore di configurazione potrebbe portare alla visualizzazione di una finestra di dialogo di sicurezza di Windows quando il sistema viene commutato da IVUS alla modalità FFR/iFR. Se l'utente risponde alla finestra di dialogo selezionando "Consenti l'accesso" ("Allow access") (come viene mostrato di seguito) le impostazioni del firewall di rete del dispositivo saranno modificate, aprendo le porte della rete a comunicazioni potenzialmente impreviste da parte della rete dell'Azienda ospedaliera a cui il dispositivo potrebbe essere connesso.



Philips Volcano
Philips Volcano, 2870 Kilgore Road, Rancho Cordova, CA 95640 USA
www.volcanocorp.com, Tel 800 228 4728, Fax 916 638 8812

VOLCANO

PHILIPS

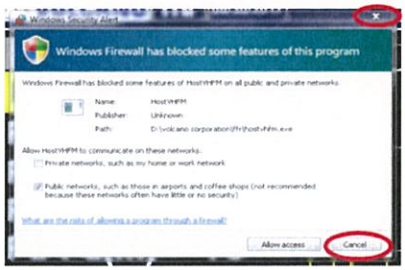
Le comunicazioni impreviste da parte della rete dell'Azienda ospedaliera potrebbero includere normali operazioni di sicurezza informatica come ad es. il port scanning. Se queste comunicazioni hanno luogo durante una procedura attiva di FFR/iFR, la registrazione dei dati potrebbe essere alterata con le seguenti conseguenze:

- Misurazioni FFR/IFR errate
- Ritardo durante la risoluzione dei problemi e/o il port scanning
- Abbandono dell'uso del sistema

Sulla base delle nostre indagini, ci sono solo alcune remote possibilità che una qualunque di queste condizioni possa verificarsi.

Philips Volcano Service eseguirà un' ispezione della configurazione del sistema nell'ambito della sua Manutenzione Preventiva o processo di servizi e correggerà la configurazione, se necessario. Ciò avrà luogo nei prossimi 12 mesi. Fino o a quel momento, potrete continuare ad utilizzare il vostro sistema purché adottiate le seguenti misure:

1. Se possibile, prima di dare inizio a una cartella del paziente, riavviate il sistema e una volta che il sistema avrà completato la sequenza di avvio, passate alla modalità FFR/iFR. Se appare la finestra di dialogo di sicurezza di Windows, selezionate "Annulla" ("Cancel") o la "X" nell'angolo in alto a destra. (Vederel'immagine di seguito)



2. Se state eseguendo una procedura potreste anche scegliere di disconnettere il Sistema Compromesso dalla rete dell'Azienda ospedaliera.

3. Se l'Allarme di Sicurezza di Windows appare sul sistema Compromesso, siete pregati di contattare i tecnici di supporto di Philips Volcano per programmare una visita di servizio per correggere questa condizione.

Qualunque cambiamento apportato alle autorizzazioni firewall effettuato selezionando "Consenti l'accesso" sarà automaticamente rimosso quando il sistema sarà riavviato. Tuttavia, l'Allarme di Sicurezza di Windows potrebbe riapparire dopo ogni successivo riavvio o riaccensione.

Siete pregati di assicurarvi che una copia di questa lettera sia fornita a tutto il personale della vostra organizzazione che gestisce questi prodotti. Siete pregati di completare, firmare e restituire il modulo accluso indicando ricezione da parte vostra di questo avviso di Azione in Situ.

Philips Volcano
Philips Volcano, 2870 Kilgore Road, Rancho Cordova, CA 95670 USA
www.volcanocorp.com, Tel 800 228 4728, Fax 916 638 8812

VOLCANO

PHILIPS

Comprendiamo il disagio che tutto ciò potrebbe arrecare a Voi, al vostro staff e ai vostri pazienti. Tuttavia, questa azione riflette l'impegno di Philips nei riguardi della sicurezza dei pazienti e del più altro standard qualitativo.

Vi ringraziamo per la vostra solerte attenzione a questa importante questione. Da parte di Philips, apprezziamo la vostra collaborazione e il vostro costante supporto.

In fede,

Peter Dekempeneer
QA & RA Manager International

Philips Volcano
Philips Volcano, 2870 Kilgore Road, Rancho Cordova, CA 95670 USA
www.volcanocorp.com, Tel 800 228 4728, Fax 916 638 8812

VOLCANO

PHILIPS

MODULO DI RESTITUZIONE DEL CLIENTE

Volcano s5i/CORE/CORE Mobile systems con software v3.5;
Windows Security Issue

Azienda Ospedaliera Nome: _____

Azienda Ospedaliera Paese: _____

Azienda Ospedaliera Indirizzo: _____

E-mail: _____

Telefono: _____

Istruzioni:

1. Siete pregati di fornire le informazioni di seguito.
2. Inviare per fax a Volcano Customer Service presso (vedi lista sottostante) o per e-mail a verecall@philips.com

Svezia	• +46850127334	**Germania**	• +493221122683167
Norvegia	• +4785228735	**Austria**	• +43125367227262
Danimarca	• +4569802402	**Svizzera**	• +41225948163
Polonia	• +48123841700	**Belgio**	• +322706575
Italia	• +390459971861	**Olanda**	• +31205248304
Spagna	• +34935207112	**GB**	• +442030700489
Francia	• +33153010911	**Per tutti gli altri Paesi**	• +3226791079

_____ NO, non ho in mio possesso alcun sistema Volcano s5i/CORE/CORE Mobile con software v3.5.

_____ SI, ho in mio possesso sistemi Volcano s5i/CORE/CORE Mobile con software v3.5 e confermo ricezione di questo avviso.

Compilato da: Nome	**Firma:**	**Data:**

Domande? Siete pregati di chiamare +32 2 713 18 20.

Philips Volcano
Philips Volcano, 2870 Kilgore Road, Rancho Cordova, CA 95640 USA
www.volcanocorp.com, Tel 800 228 4728, Fax 916 638 8812

VOLCANO

Bollettino di servizio tecnico,
Finestra di dialogo di sicurezza di Windows
Controllo numero D000185325/B

Bollettino di Servizio Tecnico Numero: D000185325

Data di emissione: 21/11/2017 **Data di decorrenza del documento: 21/11/2017**

Oggetto: Finestra di dialogo di sicurezza di Windows

Prodotti compromessi:
Sistemi s5i/CORE/CORE Mobile con software v3.5 ("Sistemi Compromessi").

Scopo della comunicazione:
Informare i clienti di un problema con una finestra di dialogo di sicurezza di Windows tra i Sistemi Compromessi e la comunicazione in rete dell'azienda ospedaliera e fornire misure per risolvere il summenzionato problema.

Riassunto delle problematiche tecniche:
Volcano Corporation è venuta a conoscenza del fatto che le impostazioni di sicurezza di Microsoft Windows su un esiguo numero di Sistemi Compromessi sono state configurate in modo erroneo durante il processo di fabbricazione. Questo errore di configurazione potrebbe portare alla visualizzazione di una finestra di dialogo di sicurezza di Windows quando il sistema viene commutato da IVUS alla modalità FFR/iFR. Se l'utente risponde alla finestra di dialogo selezionando "Allow access" ("Consenti l'accesso") (come viene mostrato di seguito) le impostazioni del firewall di rete del dispositivo saranno modificate, aprendo le porte della rete a comunicazioni potenzialmente impreviste da parte della rete dell'Azienda ospedaliera a cui il dispositivo potrebbe essere connesso.

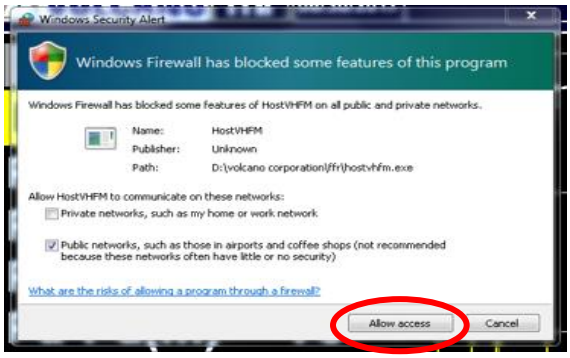


Figura 1 – Finestra di dialogo di sicurezza di Windows

Se "Allow access" ("Consenti l'accesso") è selezionato e il Sistema Compromesso incontra una comunicazione imprevista da parte della rete dell'Azienda ospedaliera durante una procedura attiva di FFR/iFR, la registrazione dei dati potrebbe essere alterata e determinare una potenziale perdita di dati che potrebbe disturbare le misurazioni dell'FFR o dell'iFR che vengono eseguite durante l'interruzione.

Se un Sistema Compromesso riceve una comunicazione imprevista da parte della rete dell'Azienda ospedaliera, si potrebbero verificare le seguenti ipotesi:

Ipotesi 1:
Sistema Compromesso: il software v3.5 esegue s5i/CORE/CORE Mobile dopo aver selezionato "Allow access" ("Consenti l'accesso") dalla finestra di dialogo di sicurezza di Windows

Quando un Sistema Compromesso riceve una comunicazione imprevista mentre è in modalità FFR/iFR dal vivo o in modalità registrazione, la visualizzazione dell'aggiornamento della pressione e delle curve ECG si fermerà brevemente e le curve risulteranno distorte (vedi **Figura 2**). Le registrazioni effettuate durante la manifestazione di questo problema non dovranno essere utilizzate.

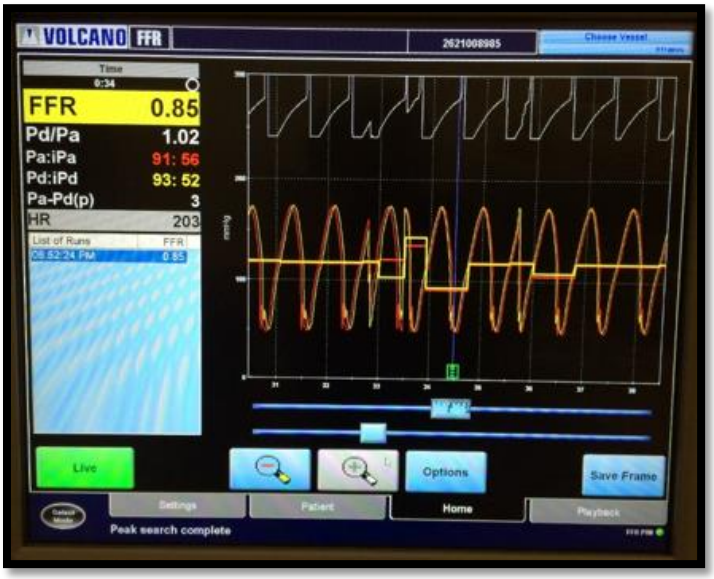


Figura 2: Schermata di FFR mentre il Sistema Compromesso riceve una comunicazione imprevista da parte della rete dell'azienda ospedaliera

Ipotesi 2
Sistemi Compromessi: 3.5 esegue s5i/CORE/CORE Mobile dopo aver selezionato "Allow access" ("Consenti l'accesso") dalla finestra di dialogo di sicurezza di Windows

Quando un Sistema Compromesso riceve dati imprevisti mentre è in modalità FFR/iFR dal vivo o in modalità registrazione, la visualizzazione dell'aggiornamento della pressione e delle curve ECG si fermerà. Le curve non verranno riaggiornate sullo schermo **(vedi FIGURA 3)**.

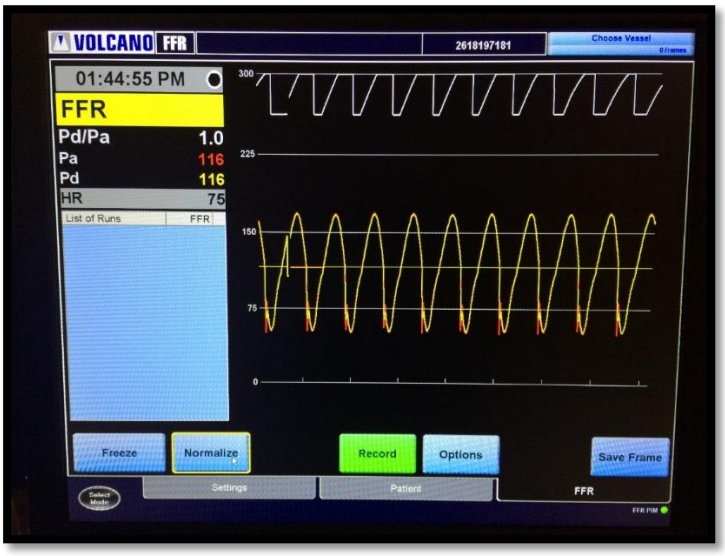


Figura 3: Schermata di FFR con la perdita delle curve di ECG e di pressione mentre il Sistema Impattato riceve una comunicazione imprevista da parte della rete dell'azienda ospedaliera

Una delle ipotesi di cui sopra potrebbe verificarsi in qualunque momento in cui tutti i seguenti pre-requisiti sono soddisfatti:

- Il sistema è acceso ed esegue un software v3.5
- Connesso via cavo a una rete dell'azienda ospedaliera
- L'utente commuta la modalità IVUS a quella FM
- Appare la finestra di dialogo Firewall
- L'utente seleziona "Allow access" ("Consenti l'accesso")
- Acquisire dati di pressione in FFR/iFR
- Comunicazione imprevista da parte della rete dell'azienda ospedaliera durante la misurazione in modalità FFR, iFR

Correzioni:

Philips Volcano Service eseguirà un'ispezione del software sul sistema nell'ambito della sua Manutenzione Preventiva o processo di servizi. Fino a quel momento, potrete continuare ad utilizzare il vostro sistema purché adottiate le seguenti misure:

1. Se possibile, prima di dare inizio a una cartella del paziente, riavviate il sistema e una volta che il sistema avrà completato la sequenza di avvio, passate alla modalità FFR/iFR. Se appare la finestra di dialogo Protezione di Windows, selezionate "Annulla" ("Cancel") o a "X" nell'angolo in alto a destra. (Figura 4)

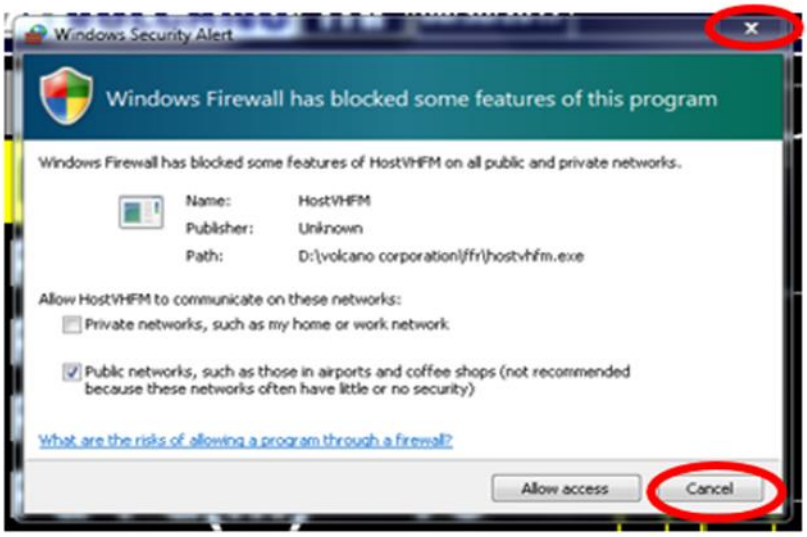


Figura 4

2. Se state eseguendo una procedura potreste anche scegliere di disconnettere il Sistema Compromesso dalla rete dell'Azienda ospedaliera. (Figura 5)
3. Se l'Allarme di Sicurezza di Windows appare sul Sistema Compromesso, siete pregati di contattare i tecnici di supporto di Philips Volcano per programmare una visita di servizio per correggere questa condizione.

Qualunque cambiamento apportato alle autorizzazioni firewall effettuato selezionando "Allow access" ("Consenti l'accesso") sarà automaticamente rimosso quando il sistema sarà riavviato. Tuttavia, l'Allarme di Sicurezza di Windows potrebbe riapparire dopo ogni successivo riavvio o riaccensione.

- **Nota:** staccare il sistema dalla rete dell'azienda ospedaliera limiterà la vostra abilità nell'utilizzo della funzione della lista di lavoro e nell'archiviare dati entro una rete PACS mentre il sistema è disconnesso dal network della struttura. Se avete necessità di riconnettere il sistema alla rete per archiviare i dati mentre non è in uso durante la procedura, assicuratevi che sia disconnesso di nuovo prima di dare avvio alla procedura.

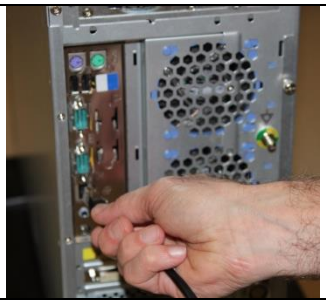
	
CORE	**CORE Mobile**
	
s5i	**s5**

Figura 5: Disconnettere il Sistema Compromesso dalla rete della struttura disconnettendo il cavo di interfaccia della rete dal pannello posteriore del sistema. In alternativa, il cavo potrà essere disconnesso da parte della struttura.

Se l'Allarme di Sicurezza di Windows appare sul Sistema Compromesso, siete pregati di contattare i tecnici di supporto di Philips Volcano per programmare una visita di servizio per correggere questa condizione.

Ulteriori considerazioni:

L'utente può ignorare la finestra di dialogo di sicurezza di Windows spostandola in un'altra sezione del monitor e continuando la procedura. Questa è una soluzione accettabile è non andrà ad influire sulla sicurezza del sistema o sull'acquisizione in FFR/iFR.

I cambiamenti alle autorizzazioni firewall saranno automaticamente rimosse quando il sistema sarà riavviato, tuttavia, la finestra di allerta sicurezza di Windows continuerà ad apparire dopo ciascun successivo riavvio. Siete pregati di contattare i tecnici del servizio in situ per correggere in modo definitivo questa condizione.

Contatti Volcano:
Per ulteriori informazioni contattare:

Volcano Corporation
2870 Kilgore Road
Rancho Cordova, CA 95670
Stati Uniti d'America
(800) 228-4728 Opzione (2)
FAX 916-358-8492

Volcano International
Technical support
Department
Excelsiorlaan 41
1930 Zaventem
Belgium
Tel: 00 32 2 713 18 20
techsupporteu@philips.com