6 aprile 2021 Inviata via mail/PEC

AVVISO URGENTE DI SICUREZZA SUL CAMPO
CORREZIONE DEL DISPOSITIVO MEDICO

Vulnerabilità della sicurezza informatica dei contropulsatori Datascope Cardiosave Hybrid e Rescue - Ripple20

PRODOTTO INTERESSATO	CODICE PRODOTTO	DATA DI DISTRIBUZIONE
Cardiosave Hybrid **Cardiosave Rescue**	**Tutti**	**Tutte**

VI PREGHIAMO DI INOLTRARE QUESTE INFORMAZIONI A TUTTI GLI ATTUALI E POTENZIALI UTENTI DEI CONTROPULSATORI CARDIOSAVE HYBRID E CARDIOSAVE RESCUE ALL'INTERNO DELLA VOSTRA STRUTTURA.

NEL CASO SIATE UN DISTRIBUTORE CHE HA SPEDITO I PRODOTTI INTERESSATI AI CLIENTI, VI PREGHIAMO DI INOLTRARE QUESTO DOCUMENTO ALLA LORO ATTENZIONE AL FINE DI AGIRE ADEGUATAMENTE.

Gentile Cliente,

Datascope/Getinge sta avviando un'azione correttiva volontaria di dispositivo medico per i contropulsatori Cardiosave Hybrid e Cardiosave Rescue a causa della vulnerabilità della sicurezza informatica in una libreria software TCP/IP di basso livello ampiamente utilizzata sviluppata da Treck, Inc. che può portare a una perdita di comunicazione con il Sistema informativo ospedaliero/Sistema informativo clinico (HIS/CIS).

L'impossibilità di trasmettere i dati della terapia e della forma d'onda dal contropulsatore Cardiosave al registro elettronico (HIS/CIS) non influisce sul trattamento acuto del paziente in supporto.

I nostri dati indicano che la vostra struttura ha ricevuto una o più unità di contropulsatori Cardiosave.

Identificazione del problema:

Il 19 giugno 2020, il laboratorio di ricerca JSOF ha pubblicato una serie di vulnerabilità di sicurezza informatica denominate Ripple20[1]. La pubblicazione consisteva in diciannove (19) vulnerabilità che interessano centinaia di milioni di dispositivi compatibili con la connessione Ethernet/Internet.

[1] https://www.jsof-tech.com/ripple20/

Getinge
45 Barbour Pond Drive
Wayne, NJ 07470 USA
www.getinge.com

L'indagine di Getinge ha rivelato che cinque (5) delle diciannove (19) vulnerabilità potrebbero interessare il sistema operativo dei contropulsatori Cardiosave. Se una qualsiasi delle vulnerabilità venisse sfruttata, la comunicazione Ethernet andrebbe persa e Cardiosave non sarebbe in grado di comunicare al Sistema informativo ospedaliero/Sistema informativo clinico (HIS/CIS) i dati della terapia e della forma d'onda.

Nonostante il mancato invio della terapia e dei dati della forma d'onda all'HIS/CIS, Cardiosave IABP continuerà ad erogare la terapia al paziente come previsto e non ci sarà alcuna riduzione delle prestazioni del dispositivo.

Le cinque vulnerabilità sono elencate nella tabella seguente:

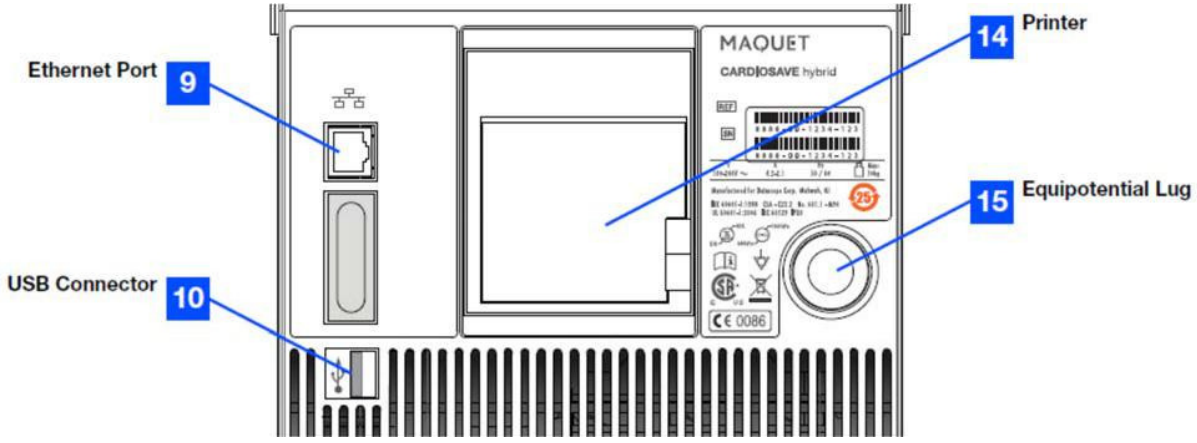
Vulnerabilità	Dettagli
CVE-2020-11896	Gestione impropria del parametro di lunghezza in IP4/UDP
CVE-2020-11906	Convalida di input non corretta nel componente Ethernet Link Layer
CVE-2020-11907	Gestione impropria dell'incoerenza dei parametri di lunghezza nel componente TCP
CVE-2020-11911	Controllo di accesso improprio in ICMPv4.
CVE-2020-11914	Convalida dell'input non corretta nel componente ARP

È importante evidenziare che non si sono verificati eventi avversi o decessi attribuibili a questo problema.

<u>Azioni Interim immediate da intraprendere da parte dell'utente:</u>

Per garantire che Cardiosave Hybrid o Cardiosave Rescue non siano suscettibili alle vulnerabilità di Ripple20, gli utenti possono scollegare il cavo Ethernet dalla porta Ethernet Cardiosave identificata con il numero 9 nella Figura 1 riportata di seguito:

Figura 1 (Retro dell'unità Cardiosave Hybrid e Cardiosave Rescue)



Inoltre, l'utente può disattivare le **Connessioni di Rete** tramite le impostazioni delle connessioni di rete nel menu **Opzioni Pompa**. Assicurarsi che l'indicatore dello Stato della connessione sia rosso dopo che le connessioni di rete sono state impostate su Off.

Per accedere ai menu delle impostazioni di rete, premere prima il tasto **Preferenze** in basso nel display per visualizzare il **Menu Preferenze**.

All'interno del **Menu Preferenze** selezionare il tasto **Opzioni Pompa** per aprire il sottomenù **Opzioni pompa**.

Una volta aperto il menu **Opzioni Pompa**, selezionare **Connessioni di Rete** per accedere alle opzioni di rete.

Selezionare il tasto **Off** e verificare che l'indicatore dello **Stato della Connessione** sia rosso.

Queste azioni isoleranno Cardiosave da qualsiasi potenziale vulnerabilità basata sulla rete esterna. Cardiosave non supporta altri tipi di connessione di rete diversi dai cavi Ethernet collegati direttamente.

Azione correttiva:

Datascope/Getinge sta attualmente sviluppando una correzione software per risolvere questo problema. Un rappresentante dell'assistenza Datascope/Getinge vi contatterà per programmare l'installazione del software aggiornato. Questo lavoro sarà svolto senza alcun costo per la vostra struttura.

Vi preghiamo di completare e firmare l'allegato AVVISO URGENTE DI SICUREZZA SUL CAMPO AZIONE CORRETTIVA DI DISPOSITIVO MEDICO - MODULO DI RISPOSTA (pagina 5) per confermare di aver ricevuto questa notifica.
Restituire il modulo compilato a Datascope/Getinge inviando una copia digitalizzata a FSCA.italy@getinge.com.

Ci scusiamo per eventuali disagi causati da questa correzione del dispositivo medico.
In caso di domande, contattare il rappresentante Datascope/Getinge locale.

Questa notifica viene effettuata con la conoscenza della Food and Drug Administration statunitense.

Cordiali saluti,

Getinge
45 Barbour Pond Drive
Wayne, NJ 07470 USA

6 APRILE 2021

AVVISO URGENTE DI SICUREZZA SUL CAMPO
AZIONE CORRETTIVA DI DISPOSITIVO MEDICO
MODULO DI RISPOSTA

Vulnerabilità della sicurezza informatica dei contropulsatori Datascope Cardiosave Hybrid e Rescue - Ripple20

Restituire a FSCA.italy@getinge.com

Dichiaro di aver esaminato e compreso questo avviso urgente di azione correttiva di dispositivo medico per i contropulsatori Cardiosave interessati di questa struttura.

Confermo inoltre che tutti gli utilizzatori del contropulsatore Cardiosave presenti in questa struttura sono stati informati di conseguenza.

Rappresentante della struttura:

Firma:_____ Data:_____

Nome e Cognome: _____ Telefono: _____

Titolo: _____ Dipartimento: _____

Nome dell'ospedale: _____

Indirizzo completo: _____

Vi preghiamo di restituire il modulo compilato via e-mail a FSCA.italy@getinge.com

Getinge
45 Barbour Pond Drive
Wayne, NJ 07470 USA
www.getinge.com