Medtronic

Medtronic (Svizzera) SA
Talstrasse 9
3053 Münchenbuchsee
www.medtronic.ch

Tel. 031 868 01 00
Fax 031 868 01 99
E-Mail swisscontact@medtronic.com

Notifica pubblicazione Security Bulletin

Novembre 2019

Gentile Cliente,

Con la presente comunicazione Medtronic desidera informarvi che ha identificato potenziali vulnerabilità della sicurezza informatica nel software dei generatori elettrochirurgici Valleylab™ FT10 e Valleylab™ FX8 e delle vulnerabilità nei generatori elettrochirurgici Valleylab™ FT10 e Valleylab™ LS10. Di conseguenza, Medtronic ha pubblicato gli allegati security bulletin, che descrivono queste potenziali vulnerabilità, sul proprio sito web alla pagina dedicata: www.medtronic.com/xg-en/product-security/security-bulletins.html.

Vi chiediamo di leggere gli allegati security bulletin poiché includono importanti informazioni.

Questi security bulletin fanno riferimento ai seguenti dispositivi:

Codice	Descrizione
VLFT10GEN	Generatore elettrochirurgico Valleylab™ FT10
VLLS10GEN	Generatore elettrochirurgico Valleylab™ LS10
VLFX8GEN	Generatore elettrochirurgico Valleylab™ FX8

Vi chiediamo di informare con gli allegati security bulletin tutti i professionisti sanitari utilizzatori di tali dispositivi che operano all'interno della vostra struttura o in qualsiasi organizzazione cui i dispositivi potrebbero essere stati trasferiti.

Swissmedic - l'istituto svizzero per gli agenti terapeutici ha ricevuto una copia di questo avviso.

Medtronic ha come massima priorità garantire la sicurezza dei pazienti e la qualità e l'affidabilità dei propri dispositivi. Per qualsiasi ulteriore informazione o chiarimenti, vi invitiamo a rivolgervi al rappresentante Medtronic.

L'occasione ci è gradita per porgere i nostri migliori saluti.

Medtronic (Svizzera) SA

All.:
- Security bulletin: Vulnerabilità RFID dei generatori elettrochirurgici Valleylab™ FT10 e Valleylab™ LS10.
- Security bulletin: Vulnerabilità RSSH dei generatori elettrochirurgici Valleylab™ FT10 e Valleylab™ FX8.

Riferimento Medtronic: FA894

SECURITY BULLETIN

Vulnerabilità RFID dei generatori elettrochirurgici Valleylab™ FT10 e Valleylab™ LS10

07.11.2019

Medtronic

Riepilogo vulnerabilità

Medtronic rivede attivamente le proprie procedure di sicurezza per mitigare i rischi durante la fase di sviluppo pre-commercializzazione e durante l'uso post-commercializzazione. Attraverso tali monitoraggi e test di routine, Medtronic ha identificato delle vulnerabilità della sicurezza nei generatori elettrochirurgici Valleylab™ FT10 e Valleylab™ LS10. Questi dispositivi vengono utilizzati nelle sale operatorie per assistere chirurghi e infermieri durante le procedure chirurgiche. Queste vulnerabilità potrebbero consentire l'uso di strumenti chirurgici non autentici, ovvero dispositivi che contengono circuiti personalizzati destinati a clonare o imitare nuovi dispositivi LigaSure™, da utilizzare con il generatore elettrochirurgico, che potrebbero influire sulle prestazioni del sistema di sigillatura dei vasi sanguigni LigaSure™.

Ad oggi, nessun attacco informatico, violazioni dei dati o danni ai pazienti che abbiano interessato un dispositivo Medtronic sono stati osservati o associati a questa vulnerabilità.

Mitigazione

Medtronic raccomanda ai chirurghi e agli infermieri di continuare a utilizzare questi generatori elettrochirurgici e i dispositivi LigaSure™ associati come previsto e di effettuare l'aggiornamento alla versione più recente del software. A causa del potenziale riconoscimento da parte dei generatori di dispositivi LigaSure™ non autentici, i clienti devono assicurarsi che tutti i dispositivi LigaSure™ vengano acquistati solo da Medtronic o da distributori autorizzati Medtronic.

I clienti devono seguire costantemente buone pratiche di igiene informatica collegando i generatori elettrochirurgici FT10 e LS10 alla rete ospedaliera solo quando necessario e spegnendoli tra un utilizzo e l'altro fino a quando il nuovo aggiornamento software verrà completato.

Medtronic ha rilasciato un aggiornamento del software per il generatore Valleylab™ FT10, che mitiga questa vulnerabilità della sicurezza. **Per i generatori FT10:** l'aggiornamento è disponibile per determinate versioni. I clienti devono contattare il rappresentante Medtronic di zona per ulteriori informazioni. **Per i generatori LS10:** i clienti verranno informati quando l'aggiornamento software sarà disponibile.

Si raccomanda di effettuare l'aggiornamento per una maggiore sicurezza e un'esperienza ottimale dell'utente. È possibile continuare a utilizzare i dispositivi fino all'aggiornamento software. I clienti con più generatori Valleylab™ dovranno aggiornare ogni singolo generatore.

Per qualsiasi ulteriore informazione o chiarimenti, rivolgersi al rappresentante Medtronic di zona. Se si sospetta che si sia verificata un'attività correlata alla sicurezza informatica del dispositivo, contattare Medtronic.

SECURITY BULLETIN

Vulnerabilità RSSH dei generatori elettrochirurgici Valleylab™ FT10 e Valleylab™ FX8

07.11.2019

Medtronic

Riepilogo vulnerabilità

Medtronic rivede attivamente le proprie procedure di sicurezza per mitigare i rischi durante la fase di sviluppo pre-commercializzazione e durante l'uso post-commercializzazione. Attraverso tali monitoraggi e test di routine, Medtronic ha identificato delle vulnerabilità della sicurezza nel software dei generatori elettrochirurgici Valleylab™ FT10 e Valleylab™ FX8. Questi dispositivi vengono utilizzati nelle sale operatorie per assistere chirurghi e infermieri durante le procedure chirurgiche. Queste vulnerabilità potrebbero consentire l'uso di un generatore elettrochirurgico da parte di personale non autorizzato, attraverso la rete o attraverso l'accesso fisico al dispositivo, e conseguente modifica di varie impostazioni.

Ad oggi, nessun attacco informatico, violazioni dei dati o danni ai pazienti che abbiano interessato un dispositivo Medtronic sono stati osservati o associati a questa vulnerabilità.

Mitigazione

Medtronic raccomanda ai chirurghi e agli infermieri di utilizzare questi dispositivi come previsto.

I clienti devono seguire costantemente buone procedure di igiene informatica collegando questi dispositivi alla rete ospedaliera solo quando necessario e spegnendoli tra un utilizzo e l'altro fino a quando il nuovo aggiornamento software verrà completato.

Medtronic ha aggiunto miglioramenti della sicurezza in un aggiornamento software, che mitigheranno le vulnerabilità della sicurezza identificate e proteggeranno il dispositivo Valleylab™ da intrusioni malevoli. **Per i generatori FT10:** l'aggiornamento è disponibile per determinate versioni. I clienti devono contattare il rappresentante Medtronic di zona per ulteriori informazioni. **Per i generatori FX8:** i clienti verranno informati quando l'aggiornamento software sarà disponibile.

Si raccomanda di effettuare l'aggiornamento per una maggiore sicurezza e un'esperienza ottimale dell'utente. È possibile continuare a utilizzare i dispositivi fino all'aggiornamento software. I clienti con più generatori Valleylab™ dovranno aggiornare ogni singolo generatore.

Per qualsiasi ulteriore informazione o chiarimenti, rivolgersi al rappresentante Medtronic di zona. Se si sospetta che si sia verificata un'attività correlata alla sicurezza informatica del dispositivo, contattare Medtronic.