Medtronic

Medtronic (Schweiz) AG
Talstrasse 9
3053 Münchenbuchsee
www.medtronic.ch

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

Benachrichtigung zu Sicherheitsmitteilungen

November 2019

Sehr geehrte Kundin, sehr geehrter Kunde

Mit diesem Schreiben möchten wir Sie darüber informieren, dass Medtronic potenzielle Cybersicherheitslücken in der Software der Valleylab™ FT10 und Valleylab™ FX8 elektrochirurgischen Generatoren und Sicherheitslücken in unseren Valleylab™ FT10 und Valleylab™ LS10 elektrochirurgischen Generatoren festgestellt hat. Infolgedessen haben wir die beigefügten Sicherheitsmitteilungen mit einer Beschreibung dieser potenziellen Probleme auf der öffentlich zugänglichen Medtronic Website veröffentlicht www.medtronic.com/xg-en/product-security/security-bulletins.html.

Wir bitten Sie, die Mitteilungen im Anhang, welche wichtige Informationen für unsere Kunden enthalten, zu lesen. Diese Sicherheitsmitteilungen beziehen sich auf die unten aufgeführten Artikel:

Artikelcode	Beschreibung
VLFT10GEN	Valleylab™ FT10 elektrochirurgischer Generator
VLLS10GEN	Valleylab™ LS10 elektrochirurgischer Generator
VLFX8GEN	Valleylab™ FX8 elektrochirurgischer Generator

Bitte stellen Sie sicher, dass alle Anwender der genannten Produkte und sonstige zu informierende Personen in Ihrer Organisation Kenntnis von dieser dringenden Sicherheitsinformation erhalten. Sofern Sie die Produkte an Dritte abgegeben haben, leiten Sie bitte eine Kopie dieser Information weiter.

Swissmedic – das Schweizerische Heilmittelinstitut hat eine Kopie dieser dringenden Sicherheitsinformation erhalten.

Medtronic legt bei seinen Produkten grössten Wert auf einzigartige Qualität, Zuverlässigkeit, Sicherheit und Patientensicherheit. Sollten Sie Fragen zu den angehängten Mitteilungen haben, wenden Sie sich bitte an Ihren Medtronic Repräsentanten.

Freundliche Grüsse

Medtronic (Schweiz) AG

Anlagen:
- Medtronic RFID-Sicherheitsmitteilung
- Medtronic RSSH-Sicherheitsmitteilung

Medtronic Referenz: FA894

SICHERHEITSMITTEILUNG

RFID-Sicherheitslücken bei Valleylab™ FT10 und Valleylab™ LS10 elektrochirurgischen Generatoren

07.11.2019

Medtronic

Zusammenfassung der Sicherheitslücken

Medtronic überprüft aktiv seine Sicherheitspraktiken, um Risiken während der Entwicklung vor und nach der Markteinführung zu minimieren. Im Zuge dieser routinemäßigen Überwachung und Prüfung hat Medtronic Sicherheitslücken in unseren Valleylab™ FT10 und Valleylab™ LS10 elektrochirurgischen Generatoren festgestellt. Diese Produkte werden im Operationssaal zur Unterstützung von Chirurgen und OP-Personal bei chirurgischen Eingriffen eingesetzt. Diese Sicherheitslücken könnten es ermöglichen, dass unechte chirurgische Werkzeuge, d. h. Geräte, die kundenspezifische Schaltungen zum Klonen oder Nachahmen neuer LigaSure™-Geräte enthalten, mit dem elektrochirurgischen Generator verwendet werden, was die Leistung des LigaSure™ Gefäßversiegelungssystems beeinträchtigen könnte.

Bis heute wurde noch kein Cyberangriff, keine Datenschutzverletzung oder Verletzung von Patienten durch ein Medtronic Produkt festgestellt oder mit dieser Sicherheitslücke in Verbindung gebracht.

Abhilfe

Medtronic empfiehlt Chirurgen und OP-Personal, diese elektrochirurgischen Generatoren und die dazugehörigen LigaSure™ Geräte weiterhin wie vorgesehen zu verwenden und ein Update auf die aktuelle Softwareversion vorzunehmen. Da es möglich ist, dass unechte LigaSure™ Geräte von den Generatoren erkannt werden, müssen Kunden sicherstellen, dass alle LigaSure™ Geräte nur von Medtronic oder autorisierten Medtronic Händlern gekauft werden.

Kunden sollten effektive Cybersicherheitsmaßnahmen ergreifen, indem sie die FT10 und LS10 elektrochirurgischen Generatoren nur bei Bedarf an das Krankenhausnetzwerk anschließen und zwischen den Anwendungen herunterfahren, bis das neue Software-Update abgeschlossen ist.

Medtronic hat ein Software-Update für den Valleylab™ FT10 Generator veröffentlicht, das diese Sicherheitslücke behebt. **Für die FT10 Generatoren:** Das Update ist für bestimmte Versionen verfügbar. Kunden können sich für weitere Informationen an ihren Medtronic Repräsentanten wenden. **Für die LS10 Generatoren:** Kunden werden informiert, sobald das Software-Update verfügbar ist.

Das Update wird für mehr Sicherheit und eine optimale Benutzererfahrung empfohlen. Die Geräte können bis zum Abschluss des Updates weiterverwendet werden. Kunden mit mehreren Valleylab™ Generatoren müssen jeden Generator einzeln aktualisieren.

Alle Kunden können sich für weitere Informationen an ihren lokalen Repräsentanten wenden. Wenn Sie den Verdacht haben, dass bei Ihrem Gerät problematische Cybersicherheitsaktivitäten stattgefunden haben, wenden Sie sich bitte an Medtronic.

© 2019 Medtronic. Alle Rechte vorbehalten. Medtronic, das Medtronic-Logo und Further, Together sind Markenzeichen von Medtronic.
Alle anderen Marken sind Markenzeichen eines Medtronic-Unternehmens. 11/2019 – US191074b

SICHERHEITSMITTEILUNG

RSSH-Sicherheitslücken bei Valleylab™ FT10 und Valleylab™ FX8 elektrochirurgischen Generatoren

07.11.2019

Medtronic

Zusammenfassung der Sicherheitslücken

Medtronic überprüft aktiv seine Sicherheitspraktiken, um Risiken während der Entwicklung vor und nach der Markteinführung zu minimieren. Im Zuge dieser routinemäßigen Überwachung und Prüfung hat Medtronic Sicherheitsschwachstellen in der Software der ValleylabTM FT10 und ValleylabTM FX8 elektrochirurgischen Generatoren festgestellt. Diese Produkte werden im Operationssaal zur Unterstützung von Chirurgen und OP-Personal bei chirurgischen Eingriffen eingesetzt. Diese Sicherheitslücken könnten es einer unbefugten Person ermöglichen, entweder über das Netzwerk oder durch physischen Zugriff auf das Gerät die Kontrolle über einen elektrochirurgischen Generator zu übernehmen und verschiedene Einstellungen zu ändern.

Bis heute wurde noch kein Cyberangriff, keine Datenschutzverletzung oder Verletzung von Patienten durch ein Medtronic Produkt festgestellt oder mit dieser Sicherheitslücke in Verbindung gebracht.

Abhilfe

Medtronic empfiehlt Chirurgen und OP-Personal, diese Geräte weiterhin wie vorgesehen zu verwenden.

Kunden sollten effektive Cybersicherheitsmaßnahmen ergreifen, indem sie diese Geräte nur bei Bedarf an das Krankenhausnetzwerk anschließen und zwischen den Anwendungen herunterfahren, bis das neue Software-Update abgeschlossen ist.

Medtronic hat Sicherheitsverbesserungen in ein Software-Update integriert. Diese Verbesserungen minimieren die identifizierten Sicherheitslücken und schützen das Valleylab™ Gerät vor böswilligem Zugriff. **Für die FT10 Generatoren:** Das Update ist für bestimmte Versionen verfügbar. Kunden können sich für weitere Informationen an ihren Medtronic Repräsentanten wenden. **Für die FX8 Generatoren:** Kunden werden informiert, sobald das Software-Update verfügbar ist.

Das Update wird für mehr Sicherheit und eine optimale Benutzererfahrung empfohlen. Die Geräte können bis zum Abschluss des Updates weiterverwendet werden. Kunden mit mehreren Valleylab™ Generatoren müssen jedes System einzeln aktualisieren.

Alle Kunden können sich für weitere Informationen an ihren lokalen Repräsentanten wenden. Wenn Sie den Verdacht haben, dass bei Ihrem Gerät problematische Cybersicherheitsaktivitäten stattgefunden haben, wenden Sie sich bitte an Medtronic.

© 2019 Medtronic. Alle Rechte vorbehalten. Medtronic, das Medtronic-Logo und Further, Together sind Markenzeichen von Medtronic.
Alle anderen Marken sind Markenzeichen eines Medtronic-Unternehmens. 11/2019 – US191074c