Medtronic France SAS
27 quai Alphonse Le Gallo – CS 30001
92513 Boulogne-Billancourt cedex
tél. : 01 55 38 17 00
Fax : 01 55 38 18 00
www.medtronic.com

Information Urgente de sécurité

Notification relative à la publication de bulletins de sécurité

Novembre 2019

Référence Medtronic : FA894

Bonjour,

Nous vous envoyons cette lettre afin de vous informer que Medtronic a identifié des failles de sécurité potentielles dans le logiciel des générateurs électrochirurgicaux Valleylab™ FT10 et Valleylab™ FX8, ainsi que dans les générateurs électrochirurgicaux Valleylab™ FT10 et Valleylab™ LS10. Vous trouverez en pièces jointes les bulletins de sécurité que nous avons publiés à ce sujet sur le site public de Medtronic www.medtronic.com/xg-en/product-security/security-bulletins.html.

Ces bulletins contiennent des informations importantes destinées à nos clients. Veuillez en prendre connaissance et remplir le formulaire d'accusé de réception joint à ce message.

Ces bulletins de sécurité concernent les articles répertoriés ci-dessous :

Code d'article	Description
VLFT10GEN	Générateur électrochirurgical Valleylab™ FT10
VLLS10GEN	Générateur électrochirurgical Valleylab™ LS10
VLFX8GEN	Générateur électrochirurgical Valleylab™ FX8

Medtronic s'engage à garantir une qualité et une fiabilité des produits, ainsi qu'une sécurité des patients irréprochables. Pour toute question relative aux bulletins joints, veuillez contacter votre représentant Medtronic.

Cordialement,

Emmanuel Grenon
Senior Business Unit Director Surgical Innovations France
Minimally Invasive Therapies Group (MITG)

Pièces jointes :

- Bulletin de sécurité Medtronic (RFID)
- Bulletin de sécurité Medtronic (RSSH)

Medtronic France SAS
27 quai Alphonse Le Gallo – CS 30001
92513 Boulogne-Billancourt cedex
tél. : 01 55 38 17 00
Fax : 01 55 38 18 00
www.medtronic.com

Information de sécurité
Formulaire d'accusé de réception FA894 : une réponse est requise avant le 15 mars 2020

Notification relative à la publication de bulletins de sécurité

Veuillez remplir ce formulaire dans son intégralité.

Date : _____

Nom de la personne ayant complété ce formulaire : _____

Titre : _____

Numéro de téléphone (ligne directe) : _____

E-mail : _____

Nom de l'établissement : _____

Adresse postale : _____

Ville : _____ Code postal : _____

Pays : _____

En signant ci-dessous, je reconnais avoir lu et compris les informations fournies. Je confirme également avoir transmis cette notification urgente de sécurité à tous les services et à toutes les personnes / médecins concernés de mon établissement.

Nom (en caractères d'imprimerie)	Signature	Date

Pour toute question concernant cette information, veuillez contacter votre représentant Medtronic.

MERCI D'ENVOYER CET ACCUSÉ DE RÉCEPTION PAR E-MAIL À :
affaires.reglementaires@medtronic.com ou par fax au 01.55.38.18.91.

BULLETIN DE SÉCURITÉ

Failles RFID affectant les générateurs électrochirurgicaux Valleylab™ FT10 et Valleylab™ LS10

07/11/2019

Medtronic

Résumé des failles de sécurité

Medtronic contrôle activement ses pratiques de sécurité afin de réduire les risques lors du développement précédant la mise sur le marché de ses produits et pendant leur utilisation une fois ces derniers commercialisés. Lors de cette surveillance et de cet examen de routine, Medtronic a identifié des failles de sécurité dans ses générateurs électrochirurgicaux Valleylab™ FT10 et Valleylab™ LS10. Ces appareils sont utilisés dans les blocs opératoires afin d'assister les chirurgiens et les infirmières lors des interventions chirurgicales. Ces failles de sécurité risquent de permettre l'utilisation d'outils chirurgicaux non authentiques (à savoir, des appareils contenant des circuits personnalisés dont le but est de cloner ou d'imiter les nouveaux produits LigaSure™) avec le générateur électrochirurgical, ce qui pourrait avoir une incidence sur les performances du système de ligature vasculaire LigaSure™.

À ce jour, aucune cyberattaque, aucune violation de données ni aucune blessure sur des patients impliquant un produit Medtronic n'ont été observées ou associées à cette faille.

Limitation des risques

Medtronic recommande aux chirurgiens et aux infirmières de continuer à se servir de ces générateurs électrochirurgicaux et les appareils LigaSure™ associés selon l'utilisation prévue, et d'effectuer la mise à jour logicielle. Dans la mesure où des systèmes LigaSure™ non authentiques pourraient être reconnus par les générateurs, les clients doivent s'assurer que tous les systèmes LigaSure™ ont été uniquement achetés auprès de Medtronic ou d'un distributeur Medtronic autorisé.

Il est conseillé aux clients d'appliquer des mesures de sécurité appropriées, en connectant uniquement les générateurs FT10 et LS10 au réseau de l'hôpital lorsque cela est nécessaire, et en les arrêtant entre deux utilisations, et ce jusqu'à ce que la mise à jour logicielle soit disponible.

Medtronic a publié une mise à jour logicielle pour le générateur Valleylab™ FT10, laquelle permet de réduire les risques liés à cette faille de sécurité.
Pour les générateurs FT10 : la mise à jour est disponible pour certaines versions. Pour obtenir plus d'informations, les clients doivent contacter leur représentant commercial Medtronic.
Pour les générateurs LS10 : dès que la mise à jour logicielle sera disponible, les clients en seront informés.

Il est recommandé d'effectuer la mise à jour afin de renforcer la sécurité et d'optimiser l'expérience utilisateur. Les clients peuvent continuer à utiliser les appareils jusqu'à l'application de la mise à jour. Ceux qui disposent de plusieurs générateurs Valleylab™ devront les mettre à jour un par un.

Ressources complémentaires

Cette mise à jour logicielle corrige une faille de sécurité distincte qui affecte le générateur FT10.

Pour plus d'informations, les clients doivent contacter leur représentant Medtronic. Si vous pensez que des activités suspectes en lien avec la cybersécurité se sont produites sur votre appareil, contactez Medtronic à l'adresse affaires.reglementaires@medtronic.com

BULLETIN DE SÉCURITÉ

Failles RSSH affectant les générateurs électrochirurgicaux Valleylab™ FT10 et Valleylab™ FX8

07/11/2019

Medtronic

Résumé des failles de sécurité

Medtronic contrôle activement ses pratiques de sécurité afin de réduire les risques lors du développement précédant la mise sur le marché de ses produits, et pendant leur utilisation une fois ces derniers commercialisés. Lors de cette surveillance et de cet examen de routine, Medtronic a identifié des failles de sécurité dans le logiciel des générateurs électrochirurgicaux Valleylab™ FT10 et Valleylab™ FX8. Ces appareils sont utilisés dans les blocs opératoires afin d'assister les chirurgiens et les infirmières lors des interventions chirurgicales. Ces failles de sécurité risquent de laisser un individu non autorisé prendre le contrôle d'un générateur électrochirurgical par le biais du réseau ou d'un accès physique à l'appareil, et modifier différents paramètres.

À ce jour, aucune cyberattaque, aucune violation de données ni aucune blessure sur des patients impliquant un produit Medtronic n'ont été observées ou associées à cette faille.

Limitation des risques

Medtronic recommande aux chirurgiens et aux infirmières de continuer à se servir de ces appareils selon l'utilisation prévue.

Il est conseillé aux clients d'appliquer des mesures de sécurité appropriées, en connectant uniquement ces appareils au réseau de l'hôpital lorsque cela est nécessaire, et en les arrêtant entre deux utilisations, et ce jusqu'à ce que la mise à jour logicielle soit disponible.

Medtronic a renforcé la sécurité dans une mise à jour du logiciel. Ces améliorations vont permettre de réduire les risques liés aux failles de sécurité identifiées, et ainsi de protéger l'appareil Valleylab™ contre toute intrusion malveillante.
Pour les générateurs FT10 : la mise à jour est disponible pour certaines versions. Pour obtenir plus d'informations, les clients doivent contacter leur représentant commercial Medtronic.
Pour les générateurs FX8 : dès que la mise à jour logicielle sera disponible, les clients en seront informés.

Il est recommandé d'effectuer la mise à jour afin de renforcer la sécurité et d'optimiser l'expérience utilisateur. Les clients peuvent continuer à utiliser les appareils jusqu'à l'application de la mise à jour. Ceux qui disposent de plusieurs générateurs Valleylab™ devront les mettre à jour un par un.

Ressources complémentaires

Cette mise à jour logicielle corrige une faille de sécurité distincte qui affecte le générateur FT10.

Pour plus d'informations, les clients doivent contacter leur représentant commercial local. Si vous pensez que des activités suspectes en lien avec la cybersécurité se sont produites sur votre appareil, contactez Medtronic à l'adresse affaires.reglementaires@medtronic.com