7 mai 2021 par lettre recommandée avec accusé de réception

NOTIFICATION DE SÉCURITÉ URGENTE
ACTION CORRECTIVE SUR DISPOSITIFS MÉDICAUX

Consoles de contre-pulsion intra-aortique (CPBIA) Datascope Cardiosave Hybrid et Rescue
Vulnérabilités de cybersécurité – Ripple20

PRODUIT CONCERNÉ	RÉFÉRENCE	DATE DE DISTRIBUTION
Cardiosave Hybrid CPBIA **Cardiosave Rescue CPBIA**	Tous	Tous

VEUILLEZ TRANSMETTRE CES INFORMATIONS À TOUS LES UTILISATEURS ACTUELS ET POTENTIELS DE CPBIA CARDIOSAVE HYBRID et CARDIOSAVE RESCUE AU SEIN DE VOTRE HÔPITAL / ÉTABLISSEMENT.

SI VOUS ÊTES UN DISTRIBUTEUR ET AVEZ REDISTRIBUE DES PRODUITS CONCERNÉS PAR CETTE NOTIFICATION, VEUILLEZ TRANSMETTRE CE DOCUMENT AUX DESTINATAIRES FINAUX DES DISPOSITIFS AFIN QU'ILS PRENNENT LES MESURES QUI S'IMPOSENT.

Cher Client, Chère Cliente,

Datascope/Getinge lance une action corrective volontaire de dispositif médical pour les Consoles de contre-pulsion intra-aortique (CPBIA) Cardiosave Hybrid et Cardiosave Rescue, en raison de vulnérabilités de cybersécurité détectées dans une bibliothèque logicielle TCP/IP de bas niveau développée par Treck, Inc. lesquelles sont susceptibles de provoquer une interruption de la communication avec le Système d'information hospitalier/Système d'information clinique (HIS/CIS).

L'incapacité à transmettre des courbes et valeurs relatives au traitement, de la CPBIA Cardiosave au fichier patient informatisé (HIS/CIS) n'a pas d'incidence sur le traitement d'urgence d'un patient concerné.

Nos bases de traçabilité indiquent que votre établissement a reçu une ou plusieurs unités de CPBIA Cardiosave.

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

Identification du problème :

Le 19 juin 2020, le laboratoire de recherche JSOF a publié une série de vulnérabilités de cybersécurité connue sous le nom de Ripple20[1]. La publication comprenait dix-neuf (19) vulnérabilités, qui affectent des centaines de millions d'appareils en capacité d'établir une connexion Ethernet/Internet.

L'investigation menée par Getinge a révélé que cinq (5) des dix-neuf (19) vulnérabilités peuvent affecter le système d'exploitation des dispositifs de CPBIA Cardiosave. Dans le cas où l'une de ces vulnérabilités serait exploitée, la connexion Ethernet serait perdue et le dispositif Cardiosave ne serait pas en mesure de communiquer avec le Système d'information hospitalier/Système d'information clinique (HIS/CIS) pour transmettre les courbes et valeurs relatives au traitement.

Même si la CPBIA Cardiosave ne transmet pas les courbes et valeurs relatives au traitement au HIS/CIS, elle continuera à délivrer le traitement au patient comme prévu, sans que sa performance ne soit dégradée.

Les cinq vulnérabilités sont répertoriées dans le tableau ci-dessous :

Vulnérabilité	Détails
CVE-2020-11896	Gestion inadéquate du paramètre « longueur » dans IP4/UDP.
CVE-2020-11906	Validation non adéquate des entrées dans la couche de liaison Ethernet
CVE-2020-11907	Gestion inadéquate de l'incohérence du paramètre « longueur » dans TCP
CVE-2020-11911	Contrôle d'accès invalide dans ICMPv4.
CVE-2020-11914	Validation non adéquate des entrées dans ARP

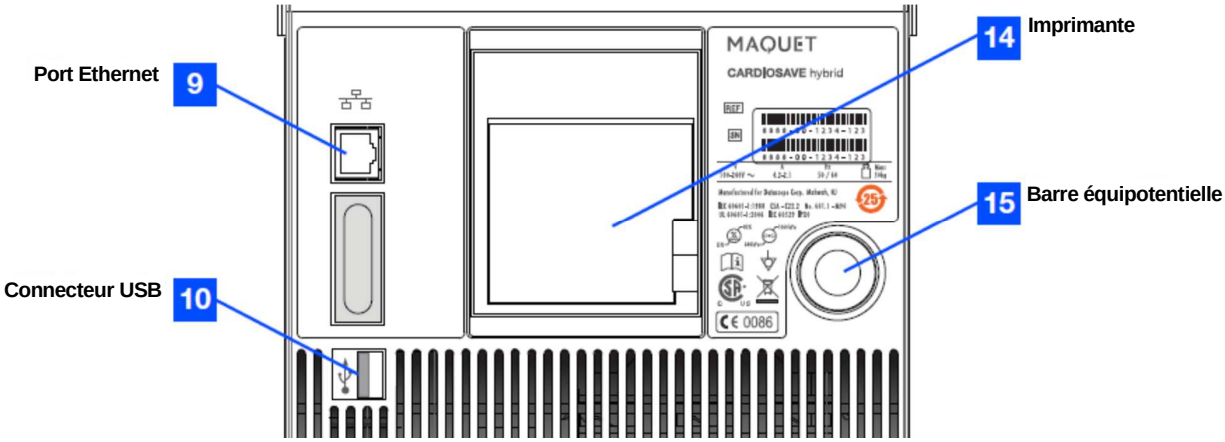
Il est important de noter qu'aucun événement indésirable ou décès n'a été attribué à ce problème.

Mesures provisoires immédiates à prendre par l'utilisateur :

Pour s'assurer que les vulnérabilités Ripple20 existantes dans les dispositifs Cardiosave Hybrid ou Cardiosave Rescue ne soient pas exploitées, les utilisateurs peuvent déconnecter le câble Ethernet du port Ethernet du Cardiosave, identifié comme élément n°9 dans l'image de la figure 1 ci-dessous :

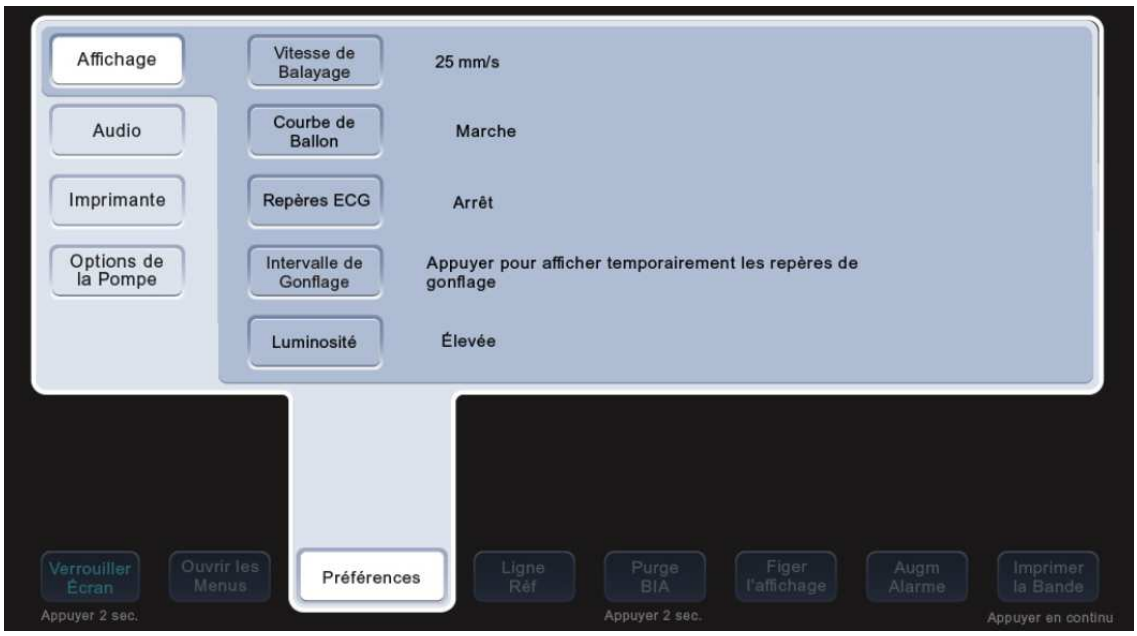
[1] https://www.jsof-tech.com/ripple20/

Figure 1 (face arrière de l'unité Cardiosave Hybrid et Cardiosave Rescue)



En outre, l'utilisateur peut désactiver les connexions réseau en configurant les **Connexions réseau** dans **Options de la Pompe**. Assurez-vous que l'indicateur État de connexion est rouge une fois les Connexions réseau désactivées.

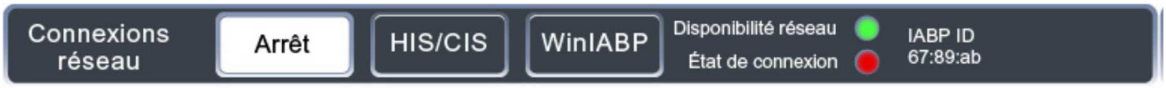
Pour accéder aux menus des paramètres réseau, appuyez d'abord sur le bouton **Préférences** sur la ligne du bas du clavier numérique pour afficher le **Menu Préférences**.



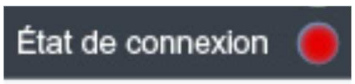
Dans le **Menu Préférences**, appuyez sur les **Options de la Pompe** pour ouvrir le sous-menu **Options pompe**.

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

Pendant que vous êtes dans le menu **Options pompe**, sélectionnez **Connexions réseau** pour accéder aux options du réseau.



Sélectionnez **Arrêt** et assurez-vous que l'indicateur **Etat de connexion** est rouge.



Ces actions isoleront le Cardiosave face aux éventuelles vulnérabilités d'un réseau externe. Le Cardiosave ne supporte pas d'autres connexions réseau que les câbles Ethernet directement connectés.

Action corrective :

Datascope/Getinge développe actuellement une mise à jour logicielle pour résoudre ce problème. Un technicien de service Datascope/Getinge vous contactera pour planifier l'installation de la mise à jour logicielle. Ces procédures seront effectuées dans votre établissement sans frais supplémentaires.

Veuillez compléter et signer le FORMULAIRE DE RÉPONSE DE LA NOTIFICATION DE SÉCURITÉ URGENTE ci-joint (page 5) afin de confirmer la bonne réception de cette communication. Retournez le formulaire complété à Datascope/Getinge en envoyant une copie scannée par courrier électronique à *qrc.fr@getinge.com*.

Nous tenons à nous excuser pour les désagréments éventuels que cette notification pourrait occasionner. Si vous avez des questions, veuillez contacter votre représentant Datascope/Getinge local.

Cette notification a également fait l'objet d'une information auprès de l'ANSM.

Cordialement,

_____
Bénédicte Parisot
Directrice QRC - Getinge France

7 mai 2021

NOTIFICATION DE SÉCURITÉ URGENTE
ACTION CORRECTIVE SUR DISPOSITIFS MÉDICAUX
FORMULAIRE DE RÉPONSE

Consoles de contre-pulsion intra-aortique (CPBIA) Datascope Cardiosave Hybrid et Rescue
Vulnérabilités de cybersécurité – Ripple20

À RENVOYER PAR COURRIER ELECTRONIQUE À : *qrc.fr@getinge.com*

Par la présente, je soussigné accuse réception de la Notification de Sécurité Urgente ci-dessus mentionnée, et atteste avoir compris les actions concernant la ou les Consoles de contre-pulsion intra-aortique Cardiosave concernées au sein de cet établissement.

Je confirme que tous les utilisateurs de la ou des Consoles de contre-pulsion intra-aortique Cardiosave de cet établissement ont été informés en conséquence.

Merci de bien vouloir compléter les informations requises ci-dessous et signer ce formulaire.

Représentant de l'établissement :

Signature :_____ Date :_____

Nom :_____ Téléphone :_____

Titre :_____ Service : _____

Nom de l'Hôpital :_____

Adresse, Code Postal, Ville : _____

Veuillez retourner le formulaire complété par COURRIER ELECTRONIQUE à
qrc.fr@getinge.com

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