| Hillrom<br>Welch Allyn, Inc. 4341 State Street Road<br>Skaneateles Falls, NY 13153 USA | **Urgent : avis de sécurité** | Baxter<br>**FA-2021-12-001-MKE-004** |
|---|---|---|

**Objet :** Vulnérabilité des mots de passe avec l'authentification unique

| Nom commercial du produit concerné : | Informations relatives aux dispositifs concernés : versions logicielles concernées |
|---|---|
| Système Q-Stress® | Q-Stress – 6.x.x (toutes les versions de 6.0.0 à 6.3.1) |
| Système XScribe™ | XScribe – 5.xx à 6.xx (toutes les versions de 5.01 à 6.3.1) |
| Système HScribe™ | HScribe – 5.xx et 6.x.x (toutes les versions de 5.01 à 6.4.0) |
| Système Vision Express™ | Vision Express – 6.x.x (toutes les versions de 6.1.0 à 6.4.0) |
| Diagnostic Cardiology Suite™ (DCS) | DCS – 2.x.x (version 2.1.0) |
| ECG Connex® Cardio | Connex Cardio – 1.x.x (version 1.0.0 à 1.1.1) |
| Système RScribe™ | RScribe – 5.xx, 6.xx et 7.x.x (toutes les versions de 5.01 à 7.0.0) |

**Identifiant FCA :** FA-2021-12-001-MKE-004

**Type d'action :**
**Avis de sécurité**

---

Date :

**Destinataires :** directeur général, gestionnaire des risques d'établissement, administrateur d'établissement, ingénieur d'établissement, responsable surveillance, ingénieur biomédical, agent de liaison pour les dispositifs médicaux, directeur de la sécurité de l'information

**Description du problème :**
Hillrom a pris connaissance d'une faille logicielle concernant les dispositifs ci-dessus et qui permet la saisie de n'importe quel nom d'utilisateur enregistré dans l'application sans fournir de mot de passe. La saisie de ce nom d'utilisateur donne accès à l'application logicielle du dispositif médical avec les mêmes privilèges que le nom d'utilisateur. Cette vulnérabilité se produit uniquement lorsque l'appareil est activé par authentification unique (SSO) dans des configurations autonomes ou client/serveur.

**Risque potentiel**
Suite aux évaluations des risques de sécurité liés à ces produits, la vulnérabilité signalée est classée comme non maîtrisée, ce qui entraîne un risque résiduel inacceptable avec une moindre probabilité de blessure grave liée à des soins intensifs prodigués trop tardivement ou à un traitement inapproprié.

**Mesures à prendre par l'utilisateur :**
Veuillez désactiver l'authentification unique dans les paramètres de configuration du gestionnaire de modalités concerné. Veuillez vous reporter à l'**annexe A** ci-dessous pour obtenir des instructions relatives à la désactivation de l'authentification unique.

**Mesures devant être prises par le revendeur :**
Veuillez partager cet avis avec vos utilisateurs finaux. Contactez HillromMKE004OUS@Sedgwick.com pour recevoir une copie modifiable de cet avis. Veuillez insérer vos coordonnées sur la copie modifiable afin de permettre à vos clients de vous contacter directement.

**Personne à contacter :**
Pour toute question concernant cet avis, veuillez contacter l'assistance technique de Hillrom via l'adresse e-mail ou le numéro de téléphone ci-dessous.

| Marché/Région/Pays | Numéro de téléphone | Adresse e-mail du support technique |
|---|---|---|
| Autriche | +43 1 79567186 | emea.support@hillrom.com |
| Allemagne | +49 (0) 69 509 851 32, option 2 | emea.support@hillrom.com |
| Suisse | +41 44 6545315 | emea.support@hillrom.com |
| Royaume-Uni | +44 (0) 207 365 6780, option 2 | emea.support@hillrom.com |
| Pays-Bas | +31 (0) 20 206 13 60, option 2 | emea.support@hillrom.com |
| Espagne | +34 (0) 91 749 93 57, option 2 | emea.support@hillrom.com |
| Italie | +39 02 696 824 25, option 2 | emea.support@hillrom.com |
| France | +33 (0)1 57 32 49 94, option 2 | emea.support@hillrom.com |
| Suède | +46 (0) 85 853 65 51, option 3 | emea.support@hillrom.com |
| Irlande | +353 (0) 46 90 67 790, option 2 | emea.support@hillrom.com |
| Europe de l'Est | +353 (0) 46 90 67 790, option 2 | emea.support@hillrom.com |
| Moyen-Orient et Afrique | +353 (0) 46 90 67 790, option 2 | emea.support@hillrom.com |
| Sous-continent indien | +353 (0) 46 90 67 790, option 2 | emea.support@hillrom.com |
| Pour tous les autres pays | +353 (0) 46 90 67 790, option 2 | emea.support@hillrom.com |

**Transmission de cet avis de sécurité :**
Veuillez vous assurer que cet avis est distribué à l'ensemble du personnel concerné. Ce personnel peut inclure, sans toutefois s'y limiter, les employés et les agents des services suivants :

| | |
|---|---|
| • Les services des urgences | • Le personnel de maintenance interne |
| • Les unités de soins intensifs pour adultes | • Le personnel infirmier spécialisé en |
| • L'ensemble des services et des cliniques | • Les directeurs d'établissements de |
| • Le personnel d'ingénierie biomédicale | • Les responsables des soins infirmiers |
| • Les responsables de la gouvernance clinique | • Les unités d'oncologie |
| • Les salles d'opération ambulatoire | • Les unités de soins intensifs |
| • Les services d'ingénierie électrique et | • Les gestionnaires de risques |
| • Les magasins d'équipement et les | • Les responsables des |
| • Les responsables de la santé et de la sécurité | • Les salles d'opération |

Hillrom considère la sécurité des patients et la satisfaction de ses clients comme des priorités absolues. Nous apprécions le temps et l'attention que vous consacrez à la lecture et à la diffusion de cet avis important concernant nos produits.

## Annexe A – Consignes pour la désactivation de l'authentification unique

### Produits concernés

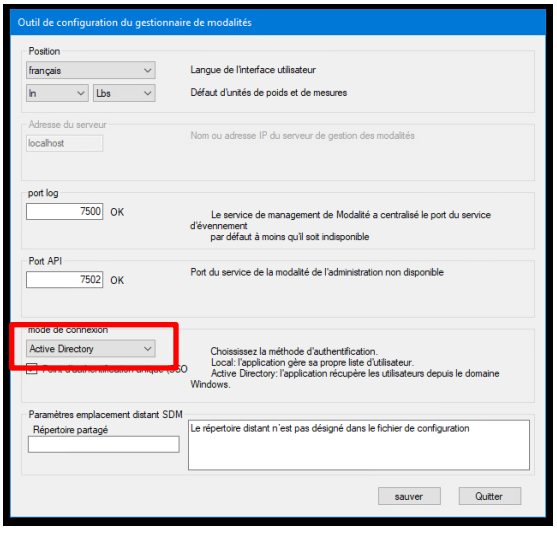
- Q-Stress 6.x.x (toutes les versions de 6.0.0 à 6.3.0) et XScribe 5.xx à 6.x.x (toutes les versions de 5.01 à 6.3.0)
- HScribe 5.xx et 6.x.x (toutes les versions de 5.01 à 6.4.0) et Vision Express 6.x.x (toutes les versions de 6.1.0 à 6.4.0)
- RScribe 5.xx, 6.x.x et 7.x.x (toutes les versions de 5.01 à 7.0.0)

### Remarques

- Ces consignes s'appliquent aux systèmes actuellement configurés avec la méthode d'authentification de connexion définie sur ***Active Directory*** et avec l'***authentification unique*** activée.
- Ce processus interrompra brièvement le service. Effectuez ces étapes à un moment approprié.
- Après avoir désactivé l'authentification unique, les utilisateurs devront saisir leur nom de compte et leur mot de passe lorsqu'ils se connecteront au système.

### Étapes à suivre pour désactiver l'authentification unique

1. Connectez-vous à Windows en tant qu'administrateur(-trice).
2. Dans le menu Start (Démarrer), accédez à ***Mortara Modality Manager*** (Gestionnaire de modalités Mortara), puis sélectionnez ***Modality Manager Configuration Tool*** *(Outil de configuration du gestionnaire de modalités).*
3. Lorsque le système vous demande d'arrêter les services, cliquez sur ***OK***.
4. La fenêtre ***Modality Manager Configuration Utility*** (Outil de configuration du gestionnaire de modalités) apparaît.




5. Assurez-vous que l'***authentification unique*** est désactivée.
6. Cliquez sur ***Save*** (Sauver), puis sur ***Exit*** (Quitter).

## Annexe A – Consignes pour la désactivation de l'authentification unique

### Produits concernés

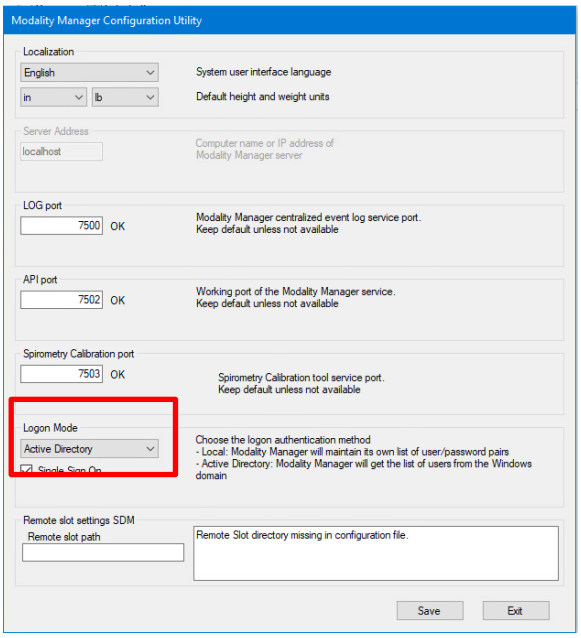
- DCS 2.x.x (version 2.1.0) et Connex Cardio 1.x.x (version 1.0.0 à 1.1.1)

### Remarques

- Ces consignes s'appliquent aux systèmes actuellement configurés avec la méthode d'authentification de connexion définie sur ***Active Directory*** et avec l'***authentification unique*** activée.
- Ce processus interrompra brièvement le service. Effectuez ces étapes à un moment approprié.
- Après avoir désactivé l'authentification unique, les utilisateurs devront saisir leur nom de compte et leur mot de passe lorsqu'ils se connecteront au système.

### Étapes à suivre pour désactiver l'authentification unique

7. Connectez-vous à Windows en tant qu'administrateur(-trice).
8. Dans le menu Start (Démarrer), accédez à ***Hillrom***, puis sélectionnez ***Connex Cardio Configuration Tool (Outil de configuration Connex Cardio)***.
9. Lorsque le système vous demande d'arrêter les services, cliquez sur ***OK***.
10. La fenêtre ***Modality Manager Configuration Utility*** (Utilitaire de configuration du gestionnaire de modalités) apparaît.




11. Assurez-vous que l'***authentification unique*** est désactivée.
12. Cliquez sur ***Save*** (Enregistrer), puis sur ***Exit*** (Quitter).

# Formulaire de réponse

**Objet :** Vulnérabilité des mots de passe avec l'authentification unique
**(FA-2021-12-001-MKE-004)**

**Il est important** que vous renvoyiez ce formulaire/reçu afin d'en accuser de réception et que vous nous fournissiez les informations nécessaires.

---

Remplissez soigneusement ce formulaire de **réponse et renvoyez -le** dans un délai de 2 semaines.

Numéro de compte Hillrom (le cas échéant) : _____

Nom de l'établissement : _____

Adresse de l'établissement : _____

Ville : _____Code postal :_____Pays : _____

Nom de la personne à contacter au sein de l'établissement (en caractères d'imprimerie) :

_____

Signature : _____ Date : _____/_____/_____

Titre :_____ Téléphone : _____

E-mail : _____

**Vérification des mesures prises** : (veuillez répondre à toutes les questions)

Nous avons lu et compris l'avis de sécurité ci-joint.
□ Oui □ Non

Les résultats de l'inspection de notre stock de produits montrent ce qui suit :
☐Nous n'avons aucun produit potentiellement concerné/Nous n'utilisons pas l'authentification unique.
☐ Des produits sont concernés. Quantité : _____ dispositifs

Nous confirmons que nous avons désactivé la l'authentification unique dans les dispositifs concernés en notre possession.
□ Oui □ Non

Uniquement à l'attention des revendeurs : nous confirmons avoir transmis cet avis à nos utilisateurs finaux :
□ Oui □ Non

Commentaires

| |
|---|
| |

Ce formulaire de réponse doit être renvoyé à l'adresse HillromMKE004OUS@Sedgwick.com dans un délai de 2 semaines.