**Assunto:** Vulnerabilidade de senha - Single Sign-On (SSO)

|  |  |
| --- | --- |
| **Nome comercial do produto afetado:** | **Detalhes sobre dispositivos afetados: versões de software afetadas** |
| Sistema Q-Stress® | Q-Stress – 6.x.x (todas as versões de 6.0.0 a 6.3.1) |
| Sistema XScribe™ | XScribe – 5.xx a 6.xx (todas as versões de 5.01 a 6.3.1) |
| Sistema HScribe™ | HScribe – 5.xx e 6.x.x (todas as versões de 5.01 a 6.4.0) |
| Sistema Vision Express™ | Vision Express – 6.x.x (todas as versões de 6.1.0 a 6.4.0) |
| Diagnostic Cardiology Suite™(DCS) | DCS – 2.x.x (versão 2.1.0) |
| Connex® Cardio ECG | Connex Cardio – 1.x.x (versão 1.0.0 a 1.1.1) |
| Sistema RScribe™ | RScribe – 5.xx, 6.xx e 7.x.x (todas as versões de 5.01 a 7.0.0) |

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

**Número da Licença na ANVISA:** 80102512463

**Tipo de ação:**

**Aviso de segurança de campo**

Data:

**Para:** Diretor executivo; Gerente de risco de instalações; Administrador de instalações; Engenheiro de instalações; Gerente de vigilância; Engenharia biomédica; Responsável pela conexão de dispositivos médicos; Diretor de segurança da informação

**Descrição do problema:**

A Hillrom tomou conhecimento de uma vulnerabilidade de software para os dispositivos acima, que permite a entrada de qualquer nome de usuário, fornecido no aplicativo, sem fornecer uma senha. A entrada desse nome de usuário concederá acesso, com os mesmos privilégios do nome de usuário, ao aplicativo de software no dispositivo médico. Essa vulnerabilidade ocorre somente quando o dispositivo é ativado com o recurso Single Sign-On (SSO) em configurações autônomas ou de cliente/servidor.

**Risco potencial**

De acordo com as avaliações de risco de segurança realizadas para os produtos, a vulnerabilidade relatada é categorizada como não controlada, resultando em risco residual inaceitável, com probabilidade improvável de lesão crítica devido ao atraso no atendimento crítico ou tratamento incorreto.

**Ações a serem tomadas pelo usuário:**

Desative o recurso SSO nas respectivas configurações do gerenciador de modalidade. Consulte o **Apêndice A** abaixo para obter instruções sobre como desabilitar o SSO.

**Ações a serem tomadas pelo distribuidor:**

Compartilhe esta notificação com seus usuários finais. Entre em contato com HillromMKE004OUS@Sedgwick.com para receber uma cópia editável desta notificação. Inclua suas informações de contato na cópia editável para permitir que seus clientes entrem em contato diretamente com você.

**Pessoa de referência para contato:**

Se você tiver alguma dúvida sobre esta notificação, entre em contato com o Suporte Técnico ou seu distribuidor da Hillrom, através do e-mail Operationsupport\_LATAM@hillrom.com ou seu distribuidor.

**Transmissão deste Aviso de Segurança de Campo:**

Certifique-se de que este aviso seja distribuído a todo o pessoal apropriado. Isso pode incluir, mas não está limitado a:

|  |  |
| --- | --- |
| * Departamentos de Acidentes e Emergências (A&E)
 | * Equipe de manutenção interna
 |
| * Unidades de terapia intensiva para adultos
 | * Especialistas em enfermagem IV
 |
| * Todas as enfermarias e clínicas
 | * Diretores médicos
 |
| * Equipe de engenharia biomédica
 | * Diretores executivos de enfermagem
 |
| * Líderes de governança clínica
 | * Unidades de oncologia
 |
| * Salas cirúrgicas ambulatoriais
 | * Unidades de terapia intensiva pediátrica
 |
| * Departamentos de Engenharia Eletrônica e Biomédica (EBME)
 | * Gestores de risco
 |
| * Lojas de equipamentos e bibliotecas
 | * Gestores de suprimentos
 |
| * Gestores de saúde e segurança
 | * Salas cirúrgicas
 |

A Hillrom considera a segurança do paciente e a satisfação do cliente nossas maiores prioridades. Agradecemos seu tempo e atenção na leitura e divulgação desta importante notificação do produto.

Atenciosamente,



Daniel Gonzalez

Diretor de Garantia de Qualidade/Assuntos Regulatórios

**Apêndice A** - **Instruções para desabilitar o Single Sign-On (SSO)**

**Produtos afetados**

* Q-Stress 6.x.x (todas as versões de 6.0.0 a 6.3.0) e XScribe 5.xx a 6.x.x (todas as versões de 5.01 a 6.3.0)
* HScribe 5.xx and 6.x.x (todas as versões de 5.01 a 6.4.0) e Vision Express 6.x.x (todas as versões de 6.1.0 a 6.4.0)
* RScribe 5.xx, 6.x.x, e 7.x.x (todas as versões de 5.01 a 7.0.0)

**Notas**

* Esta instrução é aplicável para sistemas atualmente configurados com o método de autenticação de logon definido como ***Active Directory*** e com ***Single Sign On*** (SSO) ativado.
* Este processo interromperá brevemente o serviço. Execute estas etapas em um momento apropriado.
* Depois de desativar o SSO, os usuários precisarão inserir o nome da conta e a senha ao fazer login no sistema.

**Etapas para desativar o SSO**

1. Faça login no Windows como administrador.
2. No menu Iniciar, vá para ***Gerenciador de modalidade Mortara***  e selecione ***Ferramenta de configuração do Gerenciador de modalidade****.*
3. Quando avisado que os serviços serão interrompidos, clique em ***OK****.*
4. A janela do ***Gestor de configuração da modalidade*** será exibida.



1. Certifique-se de que o ***Single Sign On*** está desativado.
2. Clique em ***Salvar*** e ***Sair***.

**Apêndice A** - **Instruções para desabilitar o Single Sign-On (SSO)**

**Produtos afetados**

* DCS 2.x.x (versão 2.1.0) e Connex Cardio 1.x.x (versão 1.0.0 a 1.1.1)

**Notas**

* Esta instrução é aplicável para sistemas atualmente configurados com o método de autenticação de logon definido como ***Active Directory*** e com ***Single Sign On*** (SSO) ativado.
* Este processo interromperá brevemente o serviço. Execute estas etapas em um momento apropriado.
* Depois de desativar o SSO, os usuários precisarão inserir o nome da conta e a senha ao fazer login no sistema.

**Etapas para desativar o SSO**

1. Faça login no Windows como administrador.
2. No menu Iniciar, vá para ***Hillrom*** e selecione ***Connex Cardio Configuration Tool***
3. Quando avisado que os serviços serão interrompidos, clique em ***OK****.*
4. A janela do ***Modality Manager Configuration Utility*** será exibida.



1. Certifique-se de que o ***Single Sign On*** está desativado.
2. Clique em ***Save*** e ***Exit***.

**Formulário de resposta**

**Assunto:** Vulnerabilidade de senha - Single Sign-On (SSO)

**(FA-2021-12-001-MKE-004)**

**É importante** que você devolva este formulário/recibo como confirmação de recebimento e nos forneça as informações necessárias.

Preencha o seguinte com as informações corretas e **devolva este Formulário de resposta** dentro de 2 semanas.

Número da conta Hillrom (se conhecido): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Nome da instalação: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Endereço da instalação: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Cidade: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_CEP:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ País: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Nome da pessoa de contato da instalação: (letra de forma) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Assinatura:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Data: \_\_\_\_\_/\_\_\_\_\_\_/\_\_\_\_\_

Cargo:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Telefone: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

E-mail: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Verificar ações tomadas**: (Por favor, não deixe nenhuma pergunta sem resposta)

Analisamos e entendemos o Aviso de Segurança de Campo anexado.

□ Sim □ Não

Os resultados da inspeção do nosso inventário de produtos mostram:

☐ Não temos produtos potencialmente afetados/Não usamos o recurso SSO.

☐ Temos produtos afetados. Quantidade: \_\_\_\_\_\_\_\_\_\_unidades.

Confirmamos que desativamos o recurso SSO nas unidades afetadas em nossa posse.

□ Sim □ Não

 Apenas para Distribuidores: Confirmamos que compartilhamos esta notificação com nossos usuários finais:

□ Sim □ Não

Comentários

|  |
| --- |
|  |

O formulário de resposta deve ser devolvido para HillromMKE004OUS@Sedgwick.com dentro de 2 semanas.