FRESENIUS KABI

Sistema de Plasmaférese AURORA

Suplemento de Segurança Cibernética

Versão do software 2.1

REF 6R4601

Rx Only

MD

471915932 (PTBR) [A] 2023/03

Índice

Introdução 1
Responsabilidade conjunta 1
Descrição do produto 2
Especificações de hardware 4
Lista de Materiais de Segurança Cibernética (CBOM) 4
Portas e serviços de rede 5
Dados confidenciais transmitidos 5
Dados confidenciais armazenados 6
Diagrama de rede e fluxo de dados 6
Proteção contra malware 7
Autenticação e autorização 7
Controles de rede 8
Criptografia 10
Registro de auditoria 10
Detecção e resposta 10
Backup e restauração 11
Conectividade remota 11
Tratamento de assistência técnica 12
Fim da vida útil e fim do período de suporte 12
Padrões de codificação segura 12
Padrões de reforço do sistema 12
Atualizações de firmware 12
Resumo de riscos 13
Operação fora do ambiente de implantação pretendido 13
Riscos residuais 13
Divulgação coordenada de vulnerabilidades (CVD) 13
Declaração de divulgação do fabricante para segurança de dispositivos médicos (MDS2) 14
Isenção de responsabilidade 14

Appendix A Lista de Materiais de Segurança Cibernética (CBOM) XML A-1

Esta página foi deixada em branco intencionalmente.

Registro do status da revisão

Número de controle do documento	Data da revisão	Número da versão do software	Revisado	Assinatura e data

Esta página foi deixada em branco intencionalmente.

Seção 1.0 Introdução

Este suplemento fornece uma visão geral das informações de segurança cibernética para o Sistema de Plasmaférese AURORA. O objetivo deste documento é detalhar como as práticas de segurança e privacidade da Fresenius Kabi foram aplicadas ao Sistema de Plasmaférese AURORA, o que o usuário deve saber sobre a manutenção da segurança deste produto e como a Fresenius Kabi pode estabelecer uma parceria com o usuário para garantir a segurança durante todo o ciclo de vida desse produto.

Este suplemento destina-se a ser usado em conjunto com o Manual do Operador do Sistema de Plasmaférese AURORA.

Seção 2.0 Responsabilidade conjunta

A segurança cibernética de dispositivos médicos é uma responsabilidade compartilhada, e isso inclui a Fresenius Kabi, o pessoal do usuário responsável pela instalação e implantação e os usuários do dispositivo.

É responsabilidade do pessoal do usuário responsável pela instalação e implantação do Sistema de Plasmaférese AURORA avaliar o nível razoável de segurança para o ambiente operacional, integrar o sistema ao ambiente operacional, fornecer a documentação necessária e treinamento aos operadores e oferecer suporte ao tratamento de incidentes de segurança.

É responsabilidade dos usuários do Sistema de Plasmaférese AURORA seguir as instruções de uso ao utilizar o Sistema de Plasmaférese AURORA, garantir que o nível de segurança exigido seja mantido (incluindo a prevenção de acesso físico ao dispositivo a usuários não autorizados) e garantir que a manutenção e as atualizações de software sejam realizadas de acordo com as recomendações da Fresenius Kabi.

A proteção abrangente do Sistema de Plasmaférese AURORA contra ameaças de segurança cibernética depende não apenas das proteções incorporadas no Sistema de Plasmaférese AURORA, mas também da segurança e proteção da rede do usuário e do ambiente ao redor. Se um ambiente de implantação seguro e protegido não puder ser fornecido, o usuário deverá informar seu representante de conta da Fresenius Kabi para desativar os recursos de conectividade do Sistema de Plasmaférese AURORA até que os requisitos neste suplemento possam ser atendidos. As medidas de proteção instaladas no próprio dispositivo (conforme detalhado neste suplemento) representam proteções administrativas, técnicas e físicas razoáveis para proteger o Sistema de Plasmaférese AURORA contra os eventos de intrusão e uso indevido mais prováveis.

À medida que os sistemas e ameaças evoluem, nenhum sistema pode ser protegido contra todas as vulnerabilidades e a Fresenius Kabi considera seus clientes os parceiros mais importantes na manutenção das proteções de segurança e privacidade. Caso tenha alguma dúvida, a Fresenius Kabi pede que todas as questões sejam trazidas ao seu conhecimento para que a empresa possa investigá-las. Quando apropriado, a Fresenius Kabi resolverá os problemas em alterações de produto, boletins técnicos e/ou divulgações responsáveis para clientes e autoridades. A Fresenius Kabi se esforça continuamente para melhorar a segurança e a privacidade em todo o ciclo de vida do produto.

Se um usuário desejar relatar um problema potencial de privacidade ou segurança relacionado ao produto (incidente, violação ou vulnerabilidade), entre em contato com a Fresenius Kabi:

Endereço: Else-Kröner-Str. 1
61352 Bad Homburg
Germany

Telefone Internacional: +49 (0) 61 72 / 686-0

Telefone dos US: 1-800-933-6925

Site: www.fresenius-kabi.com

Seção 3.0 Descrição do produto

O Sistema de Plasmaférese AURORA fornece interfaces de rede sem fio e com fio que são usadas para se comunicar com um Sistema de Gerenciamento de Dados. Um Sistema de Gerenciamento de Dados é um software que faz interface com o Sistema de Plasmaférese AURORA e permite a geração de relatórios que aumentam a produtividade, o carregamento de parâmetros de doadores e o intercâmbio de informações sobre doadores e procedimentos. O Sistema de Plasmaférese AURORA pode exportar os dados relativos ao procedimento e aos doadores que foram inseridos ou gerados durante o procedimento. Os dados exportados pelo Sistema de Plasmaférese AURORA podem ser:

- Usados para relatórios de qualidade
- Enviados para BECS (Blood Establishment Computer Software, Softwares para banco de sangue) ou um sistema de registro médico eletrônico
- Usado na criação de registros do procedimento
- Usado para eficiências operacionais

Esses dados poderão ser usados como um registro eletrônico, no lugar de determinada documentação manual, e poderão ser usados para a tomada de decisões médicas. Por outro lado, os dados podem ser usados como dados operacionais para auxiliar nas atividades comerciais, tais como a melhoria

do desempenho operacional ou da eficiência. O Sistema de Plasmaférese AURORA também pode ser configurado para ser compatível com a configuração de procedimentos remota, por meio da qual as informações do doador são enviadas e exibidas no sistema AURORA específico.

Conforme mostrado na Figura 1, a funcionalidade oferecida exige que o sistema inclua as seguintes interfaces:

- Interfaces de rede com e sem fio
- Interface do usuário (UI) com tela de toque
- Interface de porta USB para diagnóstico e manutenção
- Interface de porta USB para leitor de código de barras

As interfaces fornecidas permitem que o Sistema de Plasmaférese AURORA inclua conectividade com os seguintes acessórios opcionais:

- Servidor de Aplicação de Gerenciamento de Dados DXT, que faz interface com o Sistema de Gerenciamento de Doadores via interface de rede.
- Unidade flash USB (pen drive) via interface de porta USB para diagnóstico e manutenção.
- Leitor de código de barras via interface de porta USB para leitor de código de barras.

A interface do usuário da tela de toque implementa a Interface Homem-Máquina (IHM) para todas as interações com os usuários do Sistema de Plasmaférese AURORA.

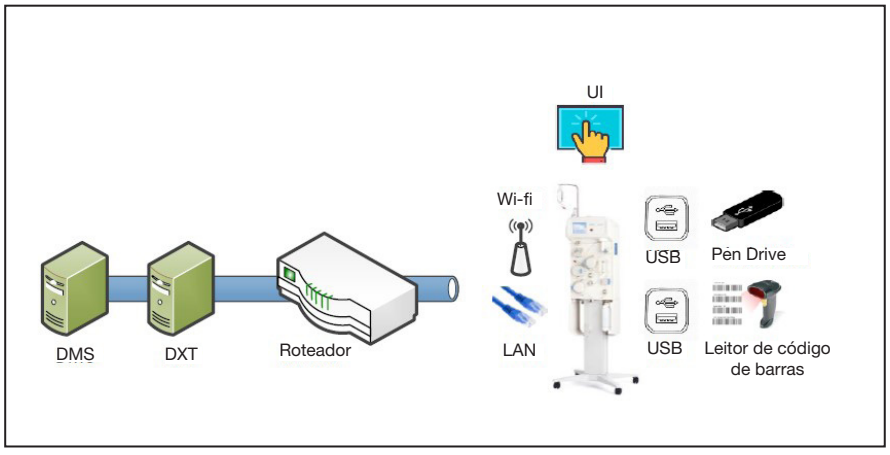

Figura 1: Produto e Acessórios

Ao isolar os recursos computacionais e os processos de doação dos processos de comunicação de rede, as funcionalidades críticas do processamento seguro do sangue foram separadas. Um ataque de segurança cibernética aos recursos de rede do Sistema de Plasmaférese AURORA por si só não afetaria a integridade ou disponibilidade do

procedimento. A separação razoável, lógica e física dos processos de interface do usuário (UI) (por exemplo, o sistema de tela de toque) dos recursos de rede também foram implementados.

Além disso, funções que fazem uso de interfaces externas, por exemplo, LAN ou USB, são projetadas para exigir confirmação de ação pelo operador na UI do Sistema de Plasmaférese AURORA. Por fim, as interfaces de rede podem ser totalmente desabilitadas para isolar o dispositivo de qualquer conectividade remota, sem qualquer impacto sobre as funções críticas de processamento de sangue. Embora a proteção completa contra todas as ameaças à segurança cibernética não seja possível sem a implementação adequada pelo cliente de uma rede e ambiente seguros e protegidos, essas medidas de isolamento oferecem proteção razoável contra as intrusões e usos indevidos mais prováveis.

Seção 4.0 Especificações de hardware

As funções de computação e conectividade do Sistema de Plasmaférese AURORA são implementadas com um Computador de Placa Única (SBC), um sistema embutido fechado. O uso de um SBC em dispositivos como o Sistema de Plasmaférese AURORA melhora muito a qualidade geral da plataforma de computação, uma vez que o design e os componentes do SBC são validados em uma escala muito maior do que o hardware proprietário de um fabricante de dispositivos de baixo volume. A funcionalidade do Sistema de Plasmaférese AURORA é compatível com as interfaces listadas na tabela a seguir:

Tabela 1: Interfaces de hardware

Interface	Especificações	Descrição
Rede com fio	IEEE 802.3	Controlador de LAN integrado
Rede sem fio	IEEE 802.11b/g	Adaptador wi-fi integrado
Código de barras Scanner	USB 2.0	Interface USB para leitores de código de barras compatíveis
Pen Drive	USB 2.0	Interface USB para pen drives compatíveis

Lista de Materiais de Segurança Cibernética (CBOM)

A Lista de Materiais de Segurança Cibernética (CBOM) pode ser fornecida mediante solicitação. Entre em contato com o representante da conta da Fresenius Kabi para saber mais.

Seção 5.0 Portas e serviços de rede

Todas as portas TCP e UDP estão permanentemente fechadas no dispositivo.

Seção 6.0 Dados confidenciais transmitidos

O Sistema de Plasmaférese AURORA transmite dois grandes conjuntos de informações pela rede de e para o Servidor de Aplicação de Gerenciamento de Dados DXT:

- Parâmetros do procedimento
- Registros do procedimento

Os parâmetros do procedimento são usados para configuração do procedimento. Alguns dos elementos de dados incluídos nos parâmetros do procedimento são:

- Identificador do procedimento
- Identificador do doador
- Peso do doador
- Altura do doador
- Sexo do doador
- Hematócrito ou hemoglobina do doador
- Perguntas de confirmação

O registro do procedimento contém os resultados do procedimento. Alguns dos elementos de dados incluídos nos parâmetros do procedimento e no registro do procedimento são:

- Identificador do procedimento
- Identificador do doador
- Peso do doador
- Altura do doador
- Hematócrito ou hemoglobina do doador

Com base nas normas e classificações de dados atuais, o acesso a essas informações, por si só, não fornece informações individualmente identificáveis a quem acessa. Essas informações podem ser usadas em conjunto com outras informações de doadores, incluindo informações recuperadas de registros manuscritos ou do sistema de gerenciamento de doadores do cliente, para identificar doadores. Como tais, os elementos de dados individuais transmitidos como parte dos parâmetros do procedimento e dos registros do procedimento não são considerados como individualmente identificáveis.

Dados confidenciais armazenados

O Sistema de Plasmaférese AURORA requer que as credenciais da rede sem fio sejam armazenadas se a conectividade com a rede for estabelecida usando a interface wi-fi do dispositivo. As credenciais da rede wi-fi são consideradas dados confidenciais, pois sua exposição não intencional pode levar a acesso não autorizado à rede sem fio. Proteções razoáveis foram implementadas para limitar o acesso às credenciais de rede armazenadas. Essas proteções incluem ocultar as credenciais de rede na tela e exigem a presença física na frente do dispositivo para acessar essas informações confidenciais.

Diagrama de rede e fluxo de dados

O ambiente recomendado para a implantação da rede, como mostrado na Figura 2, deve incluir (no mínimo) uma segurança de perímetro de rede implementada com um firewall e separação das redes locais em uma VLAN dedicada, em que os Sistemas de Plasmaférese AURORA são implantados. Se configurado corretamente, esse particionamento da rede pode proporcionar proteção contra ameaças externas e reforço no caso de comprometimento da rede corporativa.

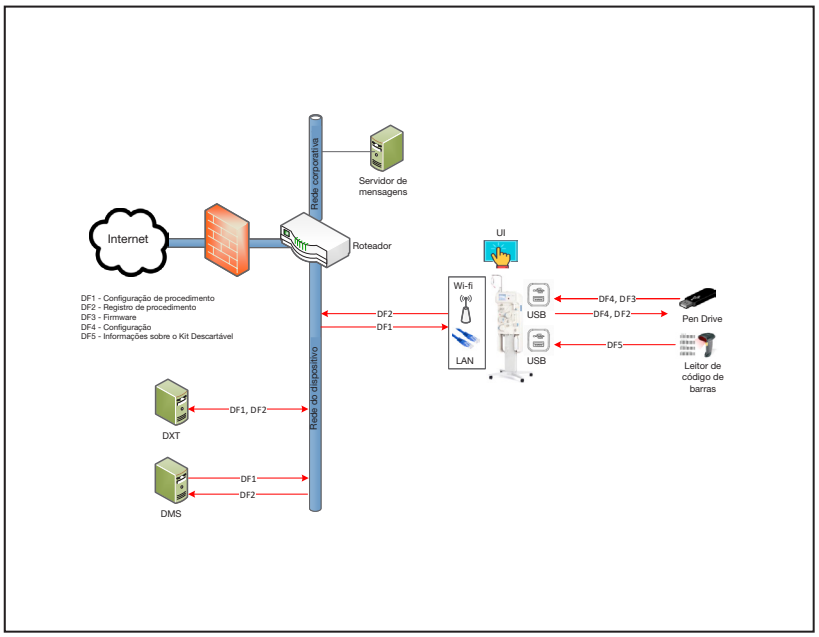

Figura 2: Diagrama de implantação

Seção 7.0 Proteção contra malware

Durante o autoteste de ativação, o Sistema de Plasmaférese AURORA realiza verificações de integridade da aplicação contra corrupção — incluindo a que pode ser causada por malware. Medidas adicionais, tais como restrições rigorosas do sistema de arquivos, estão em vigor para proteger o ambiente operacional do software do dispositivo. Como parte da responsabilidade compartilhada do cliente pela proteção de segurança cibernética, a proteção comercial antimalware/antivírus deve ser implementada na rede do Sistema de Plasmaférese AURORA e no ambiente ao redor.

Seção 8.0 Autenticação e autorização

Há três funções de usuário definidas para o funcionamento do Sistema de Plasmaférese AURORA:

- Operador

- Administrador
- Assistência técnica

A função de operador é usada para executar funções relacionadas ao uso pretendido dos dispositivos. A função de operador não inclui senha. A função pode ser configurada para inserir o identificador do operador em diferentes momentos durante o procedimento. No entanto, por padrão, essa configuração está DESATIVADA para melhorar a usabilidade.

A função de administrador é utilizada para realizar a configuração do dispositivo definida pelo usuário, como, por exemplo, os limites dos parâmetros do procedimento. A função de administrador é protegida por senha.

A função de assistência técnica é usada para executar a manutenção de rotina e os reparos necessários do dispositivo. A função de assistência técnica é protegida por senha.

Observação: Nenhuma das funções mencionadas pode usar conexão remota para acessar a funcionalidade autorizada para a função. O acesso à funcionalidade autorizada requer interação com o Sistema de Plasmaférese AURORA usando a tela de toque IHM dedicada.

Seção 9.0 Controles de rede

Os controles de rede são de responsabilidade do cliente, por exemplo, do administrador do ambiente de implantação, em conformidade com as políticas de TI do cliente que permitem o fornecimento de uma rede segura e protegida. Os controles devem ser avaliados para verificar se atendem às normas adequadas de gerenciamento de risco de segurança de redes, como a ISO/IEC 80001. As medidas de proteção padrão, como firewall e segmentação de rede, devem estar implementadas antes da implantação dos dispositivos na rede do usuário. Embora o Sistema de Plasmaférese AURORA contenha proteções rigorosas focadas no cumprimento das normas de segurança aplicáveis, por exemplo, NIST, o uso do Sistema de Plasmaférese AURORA em total cumprimento com essas normas requer o fornecimento de uma rede em conformidade e de um ambiente circundante pelo cliente.

Atenção: O Sistema de Plasmaférese AURORA e o Sistema de Gerenciamento de Dados devem ser implantados dentro de um perímetro de rede seguro para impedir o acesso de sistema(s) externo(s) não autorizado(s).

O Sistema de Plasmaférese AURORA e o Sistema de Gerenciamento de Dados devem ser implantados em um perímetro de rede seguro com as seguintes características de rede de TI:

- Compatível com IEEE 802.3 com fio 10/100 BASET Ethernet
- Compatível com LAN sem fio (consulte a tabela de configuração do adaptador de rede na seção a seguir para especificações sem fio específicas)
- Logicamente isolado e protegido de redes não confiáveis, como a Internet, ou de domínios menos confiáveis, como e-mail corporativo, por meio de dispositivos de proteção de limite (perímetro), como firewall de inspeção com estado
- Redes devidamente segmentadas, por exemplo, rede corporativa segregada (e-mail, etc.) da rede do dispositivo
- Comunicação sem fio criptografada e com integridade protegida
- Detecção de código de malware (antivírus) e/ou software de detecção de intrusão instalado e atualizado
- Capaz de rastrear e monitorar trilhas de auditoria

Observação: Os dispositivos de proteção de limite controlam o fluxo de informações entre domínios de segurança interconectados. Eles normalmente incluem gateways, roteadores, firewalls, sistemas de análise e virtualização de código malicioso baseados em rede, túneis de intrusão, interfaces gerenciadas, gateways de mensagem e gateways unidirecionais (por exemplo, diodos de dados).

Essa funcionalidade sem fio faz referência e usa os seguintes protocolos e normas do setor:

- 802.11b/g são padrões de rede sem fio desenvolvidos pelo Institute of Electrical and Electronics Engineers (IEEE). Consulte as normas ISO/IEC 8802-11 para as redes locais e de áreas metropolitanas para obter mais informações.
- WPA2/802.11i (acesso protegido à rede) é um protocolo de segurança opcional para redes sem fio. Consulte a IEEE 802.11i para obter mais informações.

Atenção: O uso de protocolos de segurança sem fio obsoletos pode aumentar os riscos de segurança cibernética associados à tentativa de um invasor de acessar ou modificar o tráfego de rede. Enquanto outros controles de defesa profunda estão em vigor para mitigar esses riscos, a Fresenius Kabi recomenda o uso de protocolos WPA2/802.11i.

- O TCP/IP (Protocolo de Controle de Transmissão/Protocolo de Internet) é um protocolo padrão de transporte de dados usado para a Internet e outras redes semelhantes. Consulte RFC 1122 para obter mais informações.

Criptografia

O Sistema de Plasmaférese AURORA se comunica com o DXT usando uma interface HTTP, que incorpora a Segurança da Camada de Transporte (TLS) com um certificado digital X.509. A Segurança da Camada de Transporte proporciona tanto a privacidade na forma de criptografia de dados quanto a integridade dos dados transferidos.

Seção 10.0 Registro de auditoria

O Sistema de Plasmaférese AURORA armazena todos os registros internamente em seu cartão de memória compacto. Os registros implementados incluem:

- Registro de eventos do sistema
- Registros do procedimento
- Registros de dados do procedimento
- Registros de execução do sistema

O acesso aos registros está disponível para todas as funções do usuário.

Os registros de procedimentos são apresentados nos formatos de arquivo XML e AVS. Eles são criados quando o operador inicia um procedimento. Eles contêm os parâmetros do procedimento, entradas do operador, identificação do operador, todos os eventos relacionados ao procedimento (com o progresso do procedimento no momento do evento) e resultados do procedimento.

O registro de eventos do sistema é um arquivo binário cíclico para registrar os principais eventos da aplicação, tais como inicialização do sistema, mudança do estado de segurança e eventos de início de procedimentos.

Seção 11.0 Detecção e resposta

Nos casos em que um evento de segurança interrompe um procedimento disparando um alerta de procedimento, o protocolo de segurança correto é executado e a notificação normalmente é exibida na interface do usuário do dispositivo.

Em todos os casos de violação de segurança, é aconselhável que o cliente isole o dispositivo comprometido de acordo com suas políticas de segurança de TI e entre em contato com a Fresenius Kabi para obter mais ajuda com o incidente.

Seção 12.0 Backup e restauração

O Sistema de Plasmaférese AURORA oferece funcionalidade de importação/exportação da configuração e dados do dispositivo por meio de uma interface USB que pode ser usada para arquivamento, retenção e restauração de dados de procedimentos críticos. O cliente pode implementar procedimentos de backup e restauração da configuração e dados do dispositivo usando essa funcionalidade para fazer backup com segurança dos componentes desejados do dispositivo e reter essas informações em caso de procedimentos de recuperação de desastres.

Seção 13.0 Conectividade remota

Como foi dito anteriormente, a proteção abrangente das funções de conectividade remota do Sistema de Plasmaférese AURORA contra ameaças de segurança cibernética depende não apenas das proteções incorporadas no Sistema de Plasmaférese AURORA, mas também da segurança e proteção da rede do cliente e do ambiente ao redor.

O Sistema de Plasmaférese AURORA não fornece o tipo tradicional de conectividade remota, como a área de trabalho remota, a qual permite o controle direto do dispositivo de uma aplicação remota.

Entretanto, o Sistema de Plasmaférese AURORA fornece uma interface para o Servidor de Aplicação de Gerenciamento de Dados DXT para receber parâmetros do procedimento de um Sistema de Gerenciamento de Doadores externo. Isso permite a substituição da entrada manual de parâmetros pelo método eletrônico, o que reduz os erros decorrentes da entrada manual de dados.

A interface para o Servidor de Aplicação de Gerenciamento de Dados DXT também é usada para relatar os resultados do procedimento no final do procedimento. Os relatórios do procedimento podem ser usados para a funcionalidade de eficiência operacional, permitindo a tendência de diferentes aspectos do procedimento para identificar áreas de melhoria na forma como o dispositivo é operado no ambiente do usuário final.

Os relatórios de procedimento também podem ser usados na funcionalidade de registro eletrônico para complementar o perfil do

doador mantido pelo sistema de gerenciamento de doadores. Essa conectividade é oferecida na interface definida anteriormente na seção Portas e serviços de rede.

Seção 14.0 Tratamento de assistência técnica

A manutenção de rotina inclui a calibração do dispositivo. Os relatórios do procedimento são recuperados do dispositivo apenas se houver um relatório indicando perda de dados ou mau funcionamento do dispositivo durante um procedimento. Como as tarefas de manutenção de rotina exigem entrada da interface do usuário por parte de usuários autenticados (o que, em circunstâncias normais, exige presença física na frente do dispositivo), essas tarefas não podem ser realizadas remotamente.

Fim da vida útil e fim do período de suporte

Não existe atualmente um fim da vida útil ou fim do suporte para o Sistema de Plasmaférese AURORA. Quando uma data de fim da vida útil for determinada para esse dispositivo ou versão de software, uma comunicação será enviada aos clientes afetados.

Padrões de codificação segura

O firmware do Sistema de Plasmaférese AURORA é desenvolvido utilizando padrões de codificação proprietários para o desenvolvimento da linguagem C, que são baseados nas boas práticas de engenharia de software. A fonte do Sistema de Plasmaférese AURORA é objeto de um rigoroso processo de revisão de código e análise estática.

Padrões de reforço do sistema

Não existem padrões de reforço implementados para o Sistema de Plasmaférese AURORA.

Seção 15.0 Atualizações de firmware

As atualizações de firmware só podem ser aplicadas pelo pessoal de serviço da Fresenius Kabi ou por indivíduos treinados e certificados pela Fresenius Kabi de acordo com o Boletim de Serviço Técnico apropriado. O usuário deve contatar seu representante de conta da Fresenius Kabi para receber atualizações de firmware para o AURORA.

Seção 16.0 Resumo de riscos

Operação fora do ambiente de implantação pretendido

A falha ao implantar o Sistema de Plasmaférese AURORA em um ambiente de implantação seguro pode aumentar a probabilidade das seguintes situações perigosas:

- Uma rede de TI segmentada ou segregada impropriamente pode tornar ineficazes os controles de segurança existentes e ser submetida a ataques cibernéticos, tais como os ataques Denial-of-Service (Negação de Serviço) ou Man-in-the-Middle (Homem no Meio).
- A falta de dispositivos de proteção de limites devidamente configurados, tais como um firewall, pode permitir que dados desnecessários ou mesmo dados prejudiciais (malware) passem ou se espalhem entre redes, o que torna os dados críticos ou sensíveis suscetíveis a monitoramento ou escuta, ou sujeitos a ataques cibernéticos.
- A falha na implementação de software antimalware nas redes de TI pode comprometer a integridade e a disponibilidade do Sistema de Plasmaférese AURORA.
- A falha no rastreamento e monitoramento adequado das trilhas de auditoria pode resultar em incidentes indetectáveis, o que pode impedir os esforços de resposta e recuperação no caso de um incidente cibernético.

Riscos residuais

Riscos residuais de segurança cibernética são divulgados no Anexo A, de acordo com os regulamentos aplicáveis e as políticas de divulgação da Fresenius Kabi.

Divulgação coordenada de vulnerabilidades (CVD)

A Fresenius Kabi divulgará todas as vulnerabilidades conhecidas de acordo com o processo de CVD.

A Fresenius Kabi aceitará os relatórios de vulnerabilidades recentemente descobertas de acordo com o processo de CVD.

Entre em contato com seu representante da Fresenius Kabi para acesso aos recursos da CVD.

Declaração de divulgação do fabricante para segurança de dispositivos médicos (MDS2)

Formulários para o Sistema de Plasmaférese AURORA podem ser fornecidos mediante solicitação. Entre em contato com o representante da conta da Fresenius Kabi para saber mais.

Isenção de responsabilidade

A Fresenius Kabi não promete ou garante aos clientes que qualquer um dos métodos ou sugestões descritos neste suplemento de segurança cibernética restaurará os sistemas do cliente, evitará erros de procedimento, resolverá quaisquer problemas relacionados a qualquer código malicioso ou proporcionará quaisquer outros resultados declarados ou pretendidos. O cliente assume exclusivamente todos os riscos relacionados ao uso ou não uso das orientações apresentadas neste Suplemento de Segurança Cibernética.

Anexo A - Lista de Materiais de Segurança Cibernética (CBOM) XML

```
<?xml version="1.0"?>
<CBOM>

        <Item>
          <Vendor>BlackBerry/QNX</Vendor>
          <Name>Neutrino RTOS</Name>
          <Version>6.5.0 SP1</Version>
          <Description>Realtime Operating System used in Aurora
          MPU</Description>
          <ThreatVectors>
            <Vector>LAN</Vector>
            <Vector>Wi-Fi</Vector>
            <Vector>USB</Vector>
            <Vector>UI</Vector>
          </ThreatVectors>
        </Item>

        <Item>
          <Vendor>BlackBerry/QNX</Vendor>
          <Name>Neutrino RTOS</Name>
          <Version>Patch 3336</Version>
          <Description>Byte Pair Encoding</Description>
          <ThreatVectors>
            <Vector>LAN</Vector>
            <Vector>Wi-Fi</Vector>
            <Vector>USB</Vector>
            <Vector>UI</Vector>
          </ThreatVectors>
        </Item>

        <Item>
          <Vendor>BlackBerry/QNX</Vendor>
          <Name>Neutrino RTOS</Name>
          <Version>Patch 3792</Version>
          <Description>Applypatch</Description>
          <ThreatVectors>
            <Vector>LAN</Vector>
            <Vector>Wi-Fi</Vector>
            <Vector>USB</Vector>
            <Vector>UI</Vector>
          </ThreatVectors>
        </Item>
```

```
        <Item>
          <Vendor>BlackBerry/QNX</Vendor>
          <Name>Neutrino RTOS</Name>
          <Version>Patch 4004</Version>
          <Description>TCP Timer</Description>
          <ThreatVectors>
            <Vector>LAN</Vector>
            <Vector>Wi-Fi</Vector>
            <Vector>USB</Vector>
            <Vector>UI</Vector>
          </ThreatVectors>
        </Item>

        <Item>
          <Vendor>BlackBerry/QNX</Vendor>
          <Name>Neutrino RTOS</Name>
          <Version>Patch 4668</Version>
          <Description>kernel libc</Description>
          <ThreatVectors>
            <Vector>LAN</Vector>
            <Vector>Wi-Fi</Vector>
            <Vector>USB</Vector>
            <Vector>UI</Vector>
          </ThreatVectors>
        </Item>

        <Item>
          <Vendor>BlackBerry/QNX</Vendor>
          <Name>Photon microGUI Library</Name>
          <Version>6.5.0</Version>
          <Description>microGUI library for creating UI</Description>
          <ThreatVectors>
            <Vector>UI</Vector>
          </ThreatVectors>
        </Item>

        <Item>
          <Vendor>BlackBerry/QNX</Vendor>
          <Name>USB stack and Library</Name>
          <Version>6.5.0</Version>
          <Description>Implements USB Protocol. Also supplies
      class drivers to communicate with USB stack</Description>
          <ThreatVectors>
            <Vector>USB</Vector>
          </ThreatVectors>
        </Item>
```

```
      <Item>
        <Vendor>GnuPG Project</Vendor>
        <Name>GnuPG</Name>
        <Version>1.4.11</Version>
        <Description>Security utility used for verifying digital
    signatures during software upgrades</Description>
        <ThreatVectors>
          <Vector>USB</Vector>
        </ThreatVectors>
      </Item>

      <Item>
        <Vendor>Expect Project</Vendor>
        <Name>Expect</Name>
        <Version>5.43.0</Version>
        <Description>Scripting language used for
    configuring network interfaces</Description>
        <ThreatVectors>
          <Vector>LAN</Vector>
          <Vector>Wi-Fi</Vector>
        </ThreatVectors>
      </Item>

      <Item>
        <Vendor>haxx</Vendor>
        <Name>libcurl</Name>
        <Version>7.19.6</Version>
        <Description>client side URL transfer library</Description>
        <ThreatVectors>
          <Vector>LAN</Vector>
          <Vector>Wi-Fi</Vector>
        </ThreatVectors>
      </Item>
</CBOM>
```

Esta página foi deixada em branco intencionalmente.

FRESENIUS KABI

Fresenius Kabi AG
Else-Kröner-Str. 1
61352 Bad Homburg / Germany
Tel.: +49 (0) 61 72 / 686-0
www.fresenius-kabi.com

Fresenius Kabi Warrendale
770 Commonwealth Drive
Warrendale, PA 15086 USA

Para US:
1-800-933-6925

US

CE 0123