FRESENIUS KABI

Sistema de aférese AmiCORE

Suplemento de segurança cibernética

SW v. 2.1

REF 6R8800

MD

471915754 (PTBR) [B] 2023/09

Índice

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 oferece uma visão geral das informações sobre segurança cibernética do sistema de aférese do AmiCORE. O objetivo deste documento é detalhar como as práticas de segurança e privacidade da Fresenius Kabi foram aplicadas ao sistema de aférese AmiCORE, o que o usuário deve saber sobre a manutenção da segurança deste produto e como a parceria da Fresenius Kabi com o usuário pode garantir a segurança em todo o ciclo de vida do produto.

Este suplemento destina-se a ser usado em conjunto com o Manual do Operador do sistema de aférese AmiCORE e o Suplemento de Gerenciamento de Dados do sistema de aférese AmiCORE.

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 aférese AmiCORE avaliar o nível razoável de segurança para o ambiente operacional, integrar o sistema ao ambiente operacional, fornecer a documentação e o treinamento necessários aos operadores e oferecer apoio para o tratamento de incidentes de segurança. É responsabilidade dos usuários seguir as instruções de uso quando utilizarem o sistema de aférese AmiCORE, garantir que o nível de segurança necessário seja mantido (incluindo o impedimento do acesso físico ao dispositivo a usuários não autorizados), bem como que a manutenção e as atualizações de software sejam realizadas de acordo com as recomendações da Fresenius Kabi.

A proteção abrangente do sistema de aférese AmiCORE contra ameaças à segurança cibernética depende não apenas das proteções integradas ao sistema de aférese AmiCORE, mas também da proteção e segurança da rede do usuário e do ambiente de instalação. Se não puder ser fornecido um ambiente de implantação seguro e protegido, o usuário deverá instruir o seu representante de conta da Fresenius Kabi para desativar os recursos de conectividade do sistema de aférese AmiCORE até que os requisitos contidos neste suplemento possam ser cumpridos. As medidas de proteção instaladas no próprio dispositivo (conforme detalhado neste suplemento) representam proteções administrativas, técnicas e físicas razoáveis para proteger o sistema de aférese AmiCORE contra os eventos mais prováveis de invasão e uso indevido.

À medida que os sistemas e ameaças evoluem, nenhum sistema pode ser protegido contra todas as vulnerabilidades e a Fresenius Kabi considera seus clientes o parceiro mais importante 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 quiser relatar um problema de privacidade ou segurança em potencial 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 para os US: 1-800-933-6925

Site: www.fresenius-kabi.com

Seção 3.0 Descrição do produto

O sistema de aférese AmiCORE 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 aférese AmiCORE e permite a geração de relatórios de aumento de produtividade, upload de parâmetros do doador/paciente e troca de informações do doador/paciente e do procedimento. O sistema de aférese AmiCORE pode exportar dados do procedimento e do doador/paciente que foram inseridos ou gerados durante o procedimento. Os dados exportados do sistema de aférese AmiCORE 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. Como alternativa, os dados poderão ser usados como dados focados operacionalmente para auxiliar nas atividades de negócios, como melhorar o desempenho ou a eficiência operacional. O sistema de aférese AmiCORE também pode ser configurado para suportar a configuração de procedimento remoto onde as informações do doador/paciente são enviadas e exibidas no sistema AmiCORE específico.

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

- Servidor de aplicação de gerenciamento de dados DXT, que faz interface com o sistema de gerenciamento de doadores via interface de rede.
- 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 aférese AmiCORE inclua conectividade com os seguintes acessórios opcionais:

- Servidor de aplicação de gerenciamento de dados DXT, que faz a 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 da tela de toque implementa uma interface homem-máquina (HMI) para todas as interações com usuários do sistema de aférese AmiCORE.

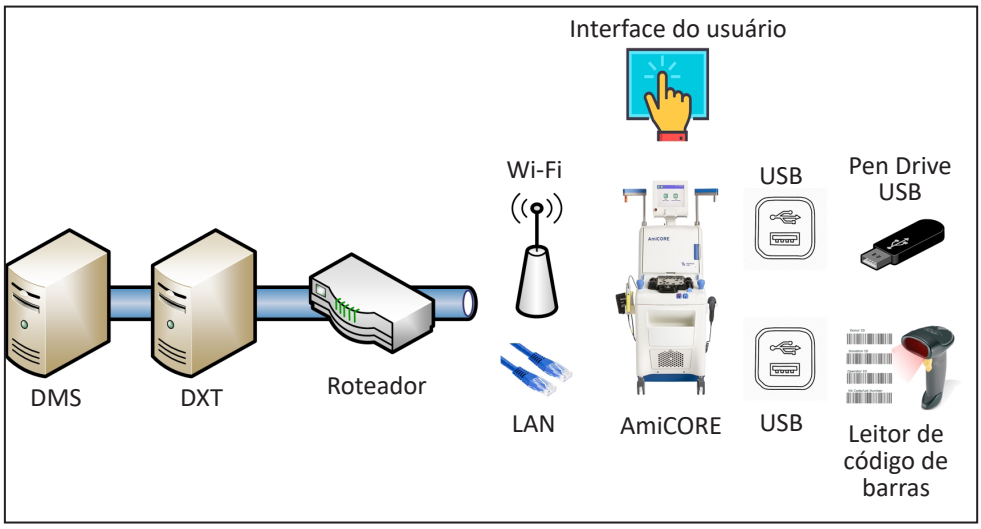


Figura 1: Produtos e acessórios

Ao isolar os recursos de computação e processos de doação dos processos de comunicação de rede, separamos as funcionalidades críticas do processamento seguro do sangue. Um ataque de segurança cibernética aos recursos de rede do sistema de aférese AmiCORE não afetaria a integridade ou disponibilidade do procedimento. A separação razoável, lógica e física dos processos de interface do usuário (UI) (por exemplo, a tela de toque) dos recursos de rede também foram implementados.

Além disso, as funções que usam interfaces externas (por exemplo, LAN ou USB) são projetadas para exigir a confirmação da ação do operador na interface do usuário do sistema de aférese AmiCORE. Por fim, as interfaces de rede podem ser totalmente desativadas para isolar o dispositivo de qualquer conectividade remota, sem afetar em nada as funções críticas do processamento de sangue. Embora a proteção completa contra todas as ameaças à segurança cibernética não seja possível sem a implementação adequada, por parte do cliente, de uma rede e ambiente de instalação seguros e protegidos, essas medidas de isolamento fornecem proteção razoável contra a invasão e usos indevidos mais prováveis.

Seção 4.0 Especificações de hardware

As funções de computação e conectividade do sistema de aférese AmiCORE são implementadas com um computador de placa única (SBC), um sistema embarcado fechado. O uso de um SBC em dispositivos como o sistema de aférese AmiCORE melhora muito a qualidade geral da plataforma computacional, pois o design e os componentes do SBC são validados em uma escala muito maior do que o hardware proprietário de fabricantes de dispositivos de baixo volume. A funcionalidade do sistema de aférese AmiCORE 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 de bordo
Leitor de código de barras	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) encontra-se nas Notas de versão para cada versão do software.

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 aférese AmiCORE recebe e transmite dois conjuntos principais de informações do servidor através da rede de e para o servidor de aplicação de gerenciamento de dados DXT:

- Parâmetros do procedimento

- Registros do procedimento

O registro do procedimento contém os resultados do procedimento. Alguns dos elementos de dados incluídos nos parâmetros do procedimento ou registro do procedimento são:

- Identificador do procedimento
- Identificador do doador
- Peso do doador
- Altura do doador
- Contagem de hematócritos do doador
- Contagem de plaquetas do doador

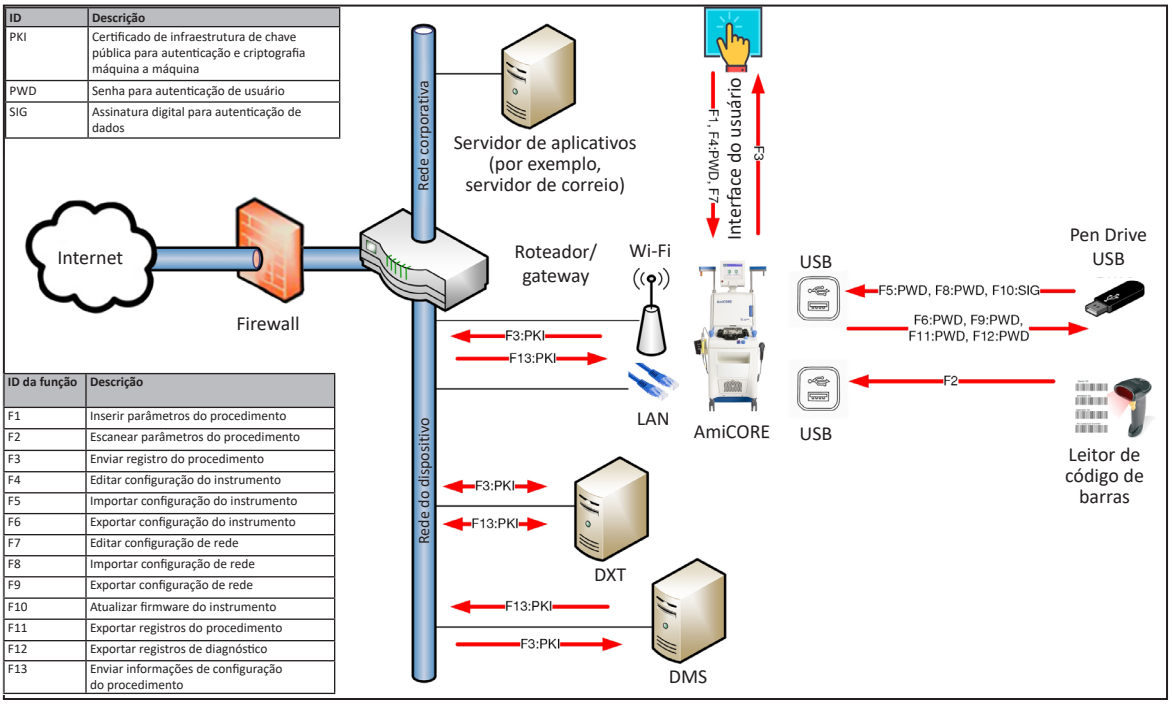
Com base nos padrões e classificações de dados atuais, o acesso a essas informações em si não fornece à parte que acessa nenhuma informação de identificação pessoal. Essas informações podem ser usadas em conjunto com outras informações do doador/paciente, incluindo informações recuperadas de registros manuscritos ou do sistema de gerenciamento de doadores/pacientes, para a identificação deles. Dessa forma, os elementos de dados individuais transmitidos como parte dos parâmetros do procedimento não são considerados informações de identificação pessoal.

Dados confidenciais armazenados

O sistema de aférese AmiCORE exige 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 de presença física na frente do dispositivo para acessar essas informações confidenciais.

Diagrama de fluxo de dados e rede

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



ID	Descrição
PKI	Certificado de infraestrutura de chave pública para autenticação e criptografia máquina a máquina
PWD	Senha para autenticação de usuário
SIG	Assinatura digital para autenticação de dados

ID da função	Descrição
F1	Inserir parâmetros do procedimento
F2	Escanear parâmetros do procedimento
F3	Enviar registro do procedimento
F4	Editar configuração do instrumento
F5	Importar configuração do instrumento
F6	Exportar configuração do instrumento
F7	Editar configuração de rede
F8	Importar configuração de rede
F9	Exportar configuração de rede
F10	Atualizar firmware do instrumento
F11	Exportar registros do procedimento
F12	Exportar registros de diagnóstico
F13	Enviar informações de configuração do procedimento

Figura 2: Diagrama de implantação

Seção 7.0 Proteção contra malware

Durante o autoteste de inicialização, o sistema de aférese AmiCORE executa verificações de integridade do sistema contra corrupção, incluindo aquelas que podem ser causadas por malware. Outras medidas, como restrições rigorosas ao sistema de arquivos, foram implementadas para proteger o ambiente do sistema operacional do dispositivo. Como parte da responsabilidade compartilhada do cliente pela proteção de segurança cibernética, a proteção antimalware/antivírus comercial deve ser implementada na rede do sistema de aférese AmiCORE e no ambiente ao redor.

Seção 8.0 Autenticação e autorização

Existem três funções de usuário definidas para a operação do sistema de aférese AmiCORE:

- 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 pode ser configurada para exigir uma senha configurável pelo usuário para acessar as funções autorizadas de administrador.

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

Observação: Nenhuma das funções mencionadas pode usar conexão remota para acessar a funcionalidade autorizada para a função. O acesso à funcionalidade autorizada para a função exige interação com o sistema de aférese AmiCORE por meio da tela de toque dedicada com interface HMI.

Seção 9.0 Controles de rede

Os controles de rede são de responsabilidade do cliente, por exemplo, do Administrador do ambiente de implantação, de acordo 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 aférese AmiCORE tenha proteções rigorosas com foco na conformidade com as normas de segurança aplicáveis, como a NIST, por exemplo, usá-lo em total conformidade com essas normas exige que o cliente forneça rede e ambiente de instalação também em conformidade.

Atenção: O sistema de aférese AmiCORE e o Sistema de Gerenciamento de Dados devem ser implantados em um perímetro de rede seguro para evitar o acesso de sistemas externos não autorizados.

O sistema de aférese AmiCORE 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 Ethernet 10/100 BASE-T IEEE802.3 com fio
- Compatível com LAN sem fio (consulte as especificações para rede sem fio na tabela de configuração do adaptador de rede)
- 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 de estados
- Redes devidamente segmentadas, por exemplo, rede corporativa segregada (e-mail, etc.) da rede do dispositivo
- Comunicação sem fio criptografada e com integridade protegida
- 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, análise de código malicioso baseado em rede e sistemas de virtualização, túneis de intrusão, interfaces gerenciadas, gateways de correio e gateways unidirecionais (por exemplo, diodos de dados).

Esta 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 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 da 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.

- 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 aférese AmiCORE se comunica com a DXT usando uma interface HTTP, que incorpora o Transport Layer Security (TLS) com um certificado digital X.509. O Transport Layer Security oferece privacidade na forma de criptografia de dados e integridade dos dados transferidos.

Seção 10.0 Registro de auditoria

O sistema de aférese AmiCORE armazena todos os registros internamente em seu cartão de memória flash 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 é limitado e depende da função do usuário.
Por exemplo:

- O operador não tem acesso aos registros.
- Administradores e usuários de serviços são os únicos usuários que podem exportar registros para uma unidade flash USB (pen drive).

Os registros do procedimento são apresentados no formato de arquivo de texto. Eles são criados quando o operador inicia um procedimento. Os registros contêm dados do procedimento, entradas do operador,

número 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 do sistema, como inicialização, mudança de estado de segurança e eventos do início de procedimento.

Seção 11.0 Detecção e resposta

Nos casos em que um evento de segurança interrompa um procedimento disparando um alerta de procedimento, o protocolo de segurança correto é executado e uma notificação normalmente é exibida na interface de usuário (IU) 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 relação ao incidente.

Seção 12.0 Backup e restauração

O sistema de aférese AmiCORE permite a funcionalidade de importação/exportação da configuração e dados do dispositivo via interface USB que pode ser usada para arquivamento, retenção e restauração de componentes essenciais do dispositivo. O cliente pode implementar procedimentos de backup e restauração para 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

Conforme explicado anteriormente, a proteção abrangente das funções de conectividade remota do sistema de aférese AmiCORE contra ameaças à segurança cibernética depende não apenas das proteções

integradas ao sistema de aférese AmiCORE, mas também da proteção e segurança da rede do cliente e do ambiente de instalação.

O sistema de aférese AmiCORE não oferece o tipo tradicional de conectividade remota, como desktop remoto, que permite o controle direto do dispositivo a partir de um aplicativo remoto. No entanto, o sistema AmiCORE fornece uma interface para o servidor de aplicação de gerenciamento de dados DXT para receber parâmetros do procedimento de um sistema externo de gerenciamento de doadores. 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 avaliar diferentes aspectos do procedimento, a fim de identificar áreas de melhoria na forma como o dispositivo é operado no ambiente do usuário final.

Os relatórios de procedimento também podem ser usados para complementar os perfis dos doadores como parte dos registros eletrônicos mantidos 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

Atualmente não há ciclo de fim da vida útil ou data de fim de período de suporte para o sistema de aférese AmiCORE. 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 aférese AmiCORE é desenvolvido usando padrões de codificação patenteados para desenvolvimento em linguagem C com base nas práticas recomendadas de engenharia de software. O sistema de aférese AmiCORE passa por rigorosos processos de revisão de código e análise estatística.

Padrões de reforço do sistema

Nenhum padrão de reforço foi implementado para o sistema de aférese AmiCORE.

Seção 15.0 Upgrades 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 entrar em contato com seu representante da conta da Fresenius Kabi para receber atualizações de firmware para o AmiCORE.

Seção 16.0 Resumo de riscos

Operação fora do ambiente de instalação pretendido

A não implantação do sistema de aférese AmiCORE em um ambiente de implantação seguro pode aumentar a probabilidade das seguintes situações de risco:

- Uma rede de TI inadequadamente segmentada ou segregada pode tornar ineficazes os controles de segurança existentes e ser submetida a ataques cibernéticos, tais como os ataques Denial-of-Service ou Man-in-the-Middle.

- A falta de dispositivos de proteção de limites devidamente configurados, como um firewall, pode permitir que dados desnecessários ou mesmo dados prejudiciais (malware) passem ou se espalhem pelas redes, o que torna os dados críticos ou sensíveis suscetíveis a monitoramento ou à escuta, ou sujeitos a ataques cibernéticos.

- A não implementação de software antimalware nas redes de TI pode comprometer a integridade e a disponibilidade do sistema de aférese AmiCORE.

- A falta de rastreamento e monitoramento adequado das trilhas de auditoria pode resultar em incidentes indetectáveis, o que pode prejudicar os esforços de resposta e recuperação no caso de um incidente cibernético.

Riscos residuais

Nenhum risco residual significativo de segurança cibernética está associado ao uso do sistema de aférese AmiCORE. Consulte o manual do operador do AmiCORE para obter informações sobre os riscos residuais associados ao uso do sistema de aférese AmiCORE como um todo.

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 um representante da Fresenius Kabi para obter acesso aos recursos de CVD ou consulte os recursos de CVD da Fresenius no site a seguir:

www.fresenius.com/vulnerability-statement

Declaração de divulgação do fabricante referente à segurança de dispositivos médicos (MDS2)

Formulários para o sistema de aférese AmiCORE podem ser fornecidos sob demanda. Entre em contato com o representante da conta da Fresenius Kabi para saber mais.

Isenção de responsabilidade

A Fresenius Kabi não promete nem 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.

FRESENIUS KABI

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

Plexus Manufacturing Sdn. Bhd.*
Plot 87, Lebuhraya Kampung Jawa
11900 Bayan Lepas
Penang, Malaysia

Feito na Malásia

Fresenius HemoCare GmbH*
Gruener Weg 10
61169 Friedberg
Germany

Feito na Alemanha

*Consulte o local de fabricação do dispositivo específico na etiqueta do instrumento.

Projetado nos EUA:

Todas as marcas exibidas pertencem aos respectivos proprietários.

CE 0123