Carestream イメージングシステム製品のサイバーセキュリティに関するガイダンス

Carestream は、品質、安全性、プライバシー、製品セキュリティの最高基準を満たす製品とサービスを顧客に提供することに尽力しています。Carestream はサイバーセキュリティを最優先課題と考え、製品のサイバーセキュリティが Carestream と顧客の間のパートナーシップにより成り立ち、それぞれが機器の操作に影響を与える悪意のある活動を防ぐ共同の責任を持つと認識しています。Carestream は、絶えず進化するサイバー脅威環境から製品を保護するために重要な予防措置を講じています。また、セキュリティ戦略の潜在的な改善点を継続的に評価し、新しいソフトウェアリリースごとに改善を実施しています。

この文書の目的は、Carestream イメージングシステムが製品とサービスを安全に運用するために講じている措置を説明することです。Carestream は、製品セキュリティが医療機器メーカー、ユーザー、およびそれらの IT 部門との共有責任であると認識しています。この文書では、機器が顧客の環境に導入された後、悪意のある活動から最大限に保護するためのさらなる推奨事項を顧客に提案しています。

製品セキュリティの強化

Carestream は、すべての製品およびサービスに含まれるソフトウェアが、インストールまたは納品時にウイルスやマルウェアがないことを保証します。

Carestream が提供するシステムは、使用されていないコンポーネントを無効化または削除することにより、デバイスの意図した使用をサポートするために必要な最小限のオペレーティングシステムのフットプリントを持つように設定されています。さらに、製品のファイアウォールは、不要なネットワークポートとプロトコルをブロックして、潜在的なマルウェア攻撃ベクトルを最小限に抑えるように構成されています。

Carestream は、医療機器の開発にセキュアソフトウェア開発ライフサイクル（SDLC）を採用しています。このプロセスでは「Secure by Design（セキュア設計）」の哲学を取り入れ、製品のプライバシーとセキュリティのトレーニング、正式な製品セキュリティ要件の設定、脅威モデリング、攻撃対象面の分析、およびプライバシーとセキュリティのリスク評価が含まれます。製品のセキュリティは、定期的なシステムセキュリティスキャン、静的コード分析、動的分析、ファズテスト、ペネトレーションテスト、および OWASP（Open Web Application Security Project）のガイドラインに基づいたコードレビューを通じて確保されます。

マルウェア対策ソフトウェア

この製品セキュリティの強化は、ゼロデイ攻撃やその他の未知の脆弱性、人的ミスに対抗するために、マルウェア対策ソフトウェアで補完すべきです。Carestream が提供しないコンピュータやオペレーティングシステムを使用して医療機器としてソフトウェアソリューション（例えば Image Suite）を使用している顧客は、サードパーティのマルウェア対策/アンチウイルスソフトウェア、ファイアウォール、その他のサイバーセキュリティ強化のベストプラクティスを使用して、侵入や感染からシステムを保護するべきです。

Carestream の DirectView および ImageView ベースの製品には、デバイスに直接統合されたホストベースの侵入防止システム（IPS）が含まれています。この IPS は、組み込みデバイス専用に特別に設計された洗練されたマルウェア防止ソリューションを提供し、従来のアンチウイルスソフトウェアよりも優れています。このシステムは、感染を事後的に除去し清掃するのではなく、積極的にマルウェアの感染を防止します。ホストベースの IPS は、既知のマルウェアやウイルスの署名を探すのではなく、システムの振る舞いやリソースへのアクセスを監視することでこれを実現します。IPS はホワイトリスト、サンドボックス化、システム強化、USB デバイス保護の組み合わせを使用して、製品をマルウェア、標的型ハッキング、内部脅威から保護します。

ホワイトリストは、システム上で実行を許可されるソフトウェアを特定するために使用されます。リストにないソフトウェアは実行できません。サンドボックス化はさらに進んで、各プログラムがどのディレクトリ、ファイル、レジストリキーを読み書きできるか、どのネットワークポートを使用できるか、どのプロセスが USB ポートや他のデバイスを使用できるかを指定します。攻撃の種類に関わらず、ポリシーベースのアプリケーションホワイトリストとヒューリスティック監視によって悪意のある活動を防止します。

標準的なアンチウイルスソフトウェアは、セキュリティ研究者がマルウェアを分析し、新しいシグネチャを生成するまで新しいマルウェアから保護することはできません。その結果、アンチウイルスソフトウェアが急速に広がるマルウェアを検出して防ぐ能力が遅れることがあります。ホストベースの侵入防止システムは、アップデートを要求せずにこのマルウェアをブロックします。この理由から、Carestream はホストベースの IPS が標準的なアンチウイルスソリューションよりも優れていると考えています。

Carestream は、ホストベースの侵入防止システム（IPS）を設定して、重要なオペレーティングシステムおよびアプリケーションファイルが変更されることがないようにし、未知のソフトウェア（アンチウイルスソフトウェアやオペレーティングシステムのパッチを含む）が、管理者権限を持つユーザーであってもインストールできないようにしています。

Carestream は、製品が承認された構成で安全かつ効果的に動作することを保証するために、広範囲にわたる検証および検証テストを実施しています。セキュリティ更新を含む、検証済みのソフトウェアのみがインストール可能です。

Carestream は、一部の顧客が自身のアンチウイルスおよびマルウェア対策ソリューションを使用することを好むことを理解しており、これによってネットワーク上のすべての情報システムを中央で監視できます。Carestream では、一部の ImageView および Image Suite システムにサードパーティのアンチウイルスおよびマルウェア対策ソフトウェアをインストールすることを許可しています。このソフトウェアが Carestream のソフトウェアを誤って悪意あるものと識別しないように、また医療機器のパフォーマンスに悪影響を及ぼさないように、適切に設定されていることが重要です。詳細については、Carestream 製品セキュリティのウェブサイトをご覧ください。

https://www.carestream.com/en/us/services-and-support/cybersecurity-and-privacy

DirectView システムにおいて、顧客がインストールしたアンチウイルスソフトウェアやその他のソフトウェアは現在サポートされていません。これらのシステムにアンチウイルスソフトウェアをインストールしようとすると、医療機器が未テストの状態になり、システムのパフォーマンスや患者の安全に悪影響を及ぼす可能性があるため、顧客はこれらのシステムにアンチウイルスソフトウェアをロードしようとする試みを避けるべきです。

継続的な監視とパッチ管理

Carestream 製品は、最新のセキュリティパッチを含むように継続的に更新されます。Carestream はセキュリティパッチと脆弱性を継続的に監視および評価し、製品構成に適用可能かどうかを判断します。Carestream には、国立脆弱性データベース（NVD）、CERT アドバイザリ、自動システムおよびソフトウェアスキャン、脆弱性開示ポリシー、およびペネトレーションテストを通じて脆弱性を監視し検出する継続的な監視プログラムがあります。さらに、Carestream は、設置された環境がリスク管理フレームワークに準拠しているかどうかを積極的に監視します。

Carestream は、製品内の管理されていない重大な脆弱性について製品セキュリティアドバイザリを公開しています。これらのアドバイザリは、H-ISAC（健康情報共有および分析センター）のアラートフィードまたは Carestream のウェブサイトで見ることができます。顧客は、新しいアドバイザリが公開され、セキュリティパッチが利用可能になったときに、自動電子メール通知を購読することもできます。

https://www.carestream.com/en/us/services-and-support/cybersecurity-and-privacy

Carestream は、医療機器にセキュリティアップデートを適用するためのいくつかの方法を提供しています。これらのツールは、セキュリティアップデートがインストールされる前に検証および承認されていることを確認します。さらに、信頼できる証明書と署名を使用して、信頼できないまたは認証されていないソースからの更新プログラムのインストールを防ぎます。

- **セキュリティ ロールアップ（SRU）ツール**：SRU ツールは、使いやすく、ワンクリックで欠落しているセキュリティ更新を自動的にインストールするツールです。単一のダウンロードで、使用されているオペレーティングシステムに関係なく、すべての DirectView および ImageView システムの最新の承認済みアップデートを提供します。SRU は Carestream のウェブサイトからダウンロードできます。
- **WSUS（Windows Server Update Services）**：Image Suite および ImageView システムには WSUS が利用可能です。Windows Update サービスを使用して、Carestream の WSUS サーバーから利用可能になった承認済みアップデートを自動的にダウンロードします。その後、ユーザーは自分の選んだ時にアップデートをインストールするように促されます。
- **その他の医療機器ソフトウェアソリューションを使用している顧客**：他の医療機器としてのソフトウェアソリューションを使用している顧客は、システムを最新のセキュリティパッチで更新し続けることを確認する必要があります。

Carestream によるマルウェアからの機器保護ガイダンス

Carestream は製品のサイバーセキュリティ戦略を継続的に評価し、ソフトウェアリリースごとにセキュリティパッチや改善を頻繁に含めています。機器の回復力を最大化するために、Carestream は顧客に対して、製品の最新のソフトウェアリリースにアップグレードすることでデバイスを最新の状態に保つことを推奨しています。

Carestream は、Carestream 機器を含むすべての医療機器を保護するために、多層的なセキュリティアプローチを適用することを強く推奨しています。推奨事項には以下が含まれますが、これらに限定されません：

- **物理的セキュリティ**：可能な場合、機器へのアクセスを物理的に制限します。
- **ロールベースのユーザーアクセス**：機器へのアクセスを許可されたユーザーのみに限定し、ロールによってユーザー権限を最小化します。
- **ネットワークの分離とセグメンテーション**：ファイアウォール、ネットワークセグメンテーション、仮想 LAN を使用し、医療機器のネットワーク通信をワークフローのサポートに必要なアドレスとポートのみに制限するように設定します。

- **ネットワーク監視**：ファイアウォール、侵入検知システム、SIEM（セキュリティ情報およびイベント管理）ログを通じてネットワーク上のデバイスの動作を監視します。

顧客はまた、Carestream のウェブサイトに公開されている製品のセキュリティおよびプライバシー情報を確認するべきです。これには以下が含まれます：

- **セキュリティおよびプライバシーに関する声明とガイドライン**
- **製品セキュリティアドバイザリ**
- **MDS2 ドキュメント**
- **セキュリティパッチとアップデート - 情報およびダウンロード**
- **ポートとプロトコルおよびファイアウォール構成**
- **サードパーティのアンチマルウェア/アンチウイルス設定情報**
- **ドメイン/Active Directory サポート**

これらのガイドラインとツールを適切に活用することで、Carestream 製品の安全性と効果性を最大限に高めることができます。

https://www.carestream.com/en/us/services-and-support/cybersecurity-and-privacy