SOLAR-OT が配備した センサー CHIYU に 関するインシデント の是正措置について

最新版ファームウェアの導入 と SOLAR-OT 監視 プラットフォーム の堅牢化

執筆者	検証者
Deirdre STARSKY, テクニカル・プロジェクト・マネージャー	Elena PIZARI, 産業部門ゼネラルマネジャー

目的

本文書は、SOLAR-OT　　が導入したアクセス管理システムのインシデント後の　　2つの是正措置を規定しています：

1. 全システムへのファームウェアアップデートの緊急展開
2. 監視プラットフォームの環境設定の強化

1. ファームウェアアップデートの緊急展開

メーカーCHIYUは、脆弱性を修正する、アクセス・コントロールの「SEMAC」システムのファームウェア・アップデートを開発しました。=>　　SOLAR-OTは緊急にこのアップデートをすべてのサイトに導入する必要があります。

以下は、SEMAC　　S2（総数の67%）に導入されるファームウェアのバージョン番号です：670VYJLN
以下は、SEMAC S3V3 (総数の 33%)に配備されるファームウェアのバージョン番号です: 628AUYSD

2. 監視プラットフォームの環境設定の強化

環境設定

その目的は、必要不可欠なサービスや機器のみを設置することで、攻撃を実行するために使用できる技術的要素を制限することです。

セキュリティのレベルを高めるには、以下を含む多くの対策が必要です：

- プラットフォームの機能制限
- プラットフォームのハードウェアの制御

A. 初期設定の変更

各コンポーネントは、以下を含む規格に従って設定されています：

- 技術アカウントと関連する認証要素
- 使用されるネットワークポート
- インストールおよび作業のリスト
- リストとファイルへのアクセス権
- サービスまたはプロセスの実行に使用されるアカウントと、このアカウントに関連する権利
- セキュリティ機能、特にトレーサビリティのための設定ファイル。

B. アクセス可能な機能の制限

プラットフォームの運用とセキュリティに不可欠なモジュールのみが維持され、適切な設定、定期的な保守、監視の対象となります。

この点に関して、オペレータは、プラットフォームの技術的運用を分析し、インストールされているが使用されていないサービスまたは機能を除外します。

各ハードウェアまたはソフトウェアの環境設定は、基準となる環境設定の形式でインベントリ化されます。

C. 接続の諸要素のインベントリ

オペレータは、プラットフォームを構成する要素の完全な技術的インベントリを実施し、それらをマッピングします。
インベントリには、プラットフォームに恒久的または一時的に、物理的またはリモートで接続できる機器（ワークステーション、サーバー、周辺機器など）が含まれます。

第三者がプラットフォームに接続する場合、オペレータはそのことをマッピングに記録し、リスク分析で考慮します。

D. 制御された諸要素の使用

オペレーターが諸要素を直接管理します。それらには以下があります：

- アップデートの展開
- 諸要素の管理
- リモートの環境設定

パーティショニング (細分化)

このプラットフォームはセグメンテーション・ロジックに従い、以下の目的のために、各サブシステムを独自のアクションに制限しています：

- 攻撃対象領域を限定する
- 可能性のある攻撃を封じ込める
- 侵害の影響を抑える
- 各サブシステムのセキュ リティレベルを適合させる

パーティショニングは物理リソースと論理リソースの両方に適用されます。

A. サブシステムへの分割

サブシステムへのセグメンテーションは以下の基準に基づいて行われます：

- 機能性
- データ保護レベル
- 暴露レベル
- セキュリティ・レベル

サブシステム間の接続は、機能的必要性によって正当化されなければなりません。

B. 物理的パーティショニング

サーバーは最も重要なアプリケーション専用になります

C. 論理的パーティショニング

サーバーに保存されるデータはすべて事前に暗号化されています。
各サブシステムは独自の暗号化メカニズムを持っています。

サブシステム間のすべての通信は、暗号化され認証された仮想プライベートネットワークを通過します。

リモートアクセス

A. パブリックアクセス

パブリックアクセスは HTTPS
プロトコルを使用し、プラットフォームはサーバー証明書の提示によって認証されます。

プラットフォーム・ユーザーに二重ファクター認証が導入されています。

B. モバイルアクセス

モバイル・ワークステーションは、プラットフォームへの認証され暗号化されたトンネルを確立するために設定されています。 トンネルを解除することができないと、インターネットやローカルネットワークにアクセスできなません。
システム・パーティションとデータ・パーティションは完全に暗号化されています。

ワークステーションに二重ファクター認証が導入されています。

ネットワーク・フィルタリング

パーティショニングに加えて、フィルタリングの仕組みを導入しています。

A. フィルタリング・ポイント

サブシステム間の相互接続は、境界フィルタリングとローカル・フィルタリングが適用される主なフィルタリング・ポイントです。

B. フィルタリング・ルール

グローバル・フローマトリックスには、有効なフィルタールールが含まれます。
それは毎年更新されます。

C. 実装

フィルタリングは、認証リストの原則に基づく専用のファイアウォールによって提供されます。