プログラマブルコントローラ CS/CJ シリーズの
ファイルシステムに対する認証の欠如の脆弱性

公開日 2023 年 04 月 17 日
オムロン株式会社

■概要

プログラマブルコントローラ CS/CJ シリーズにおいて、「重要な機能に対する認証の欠如（CWE-306）」に関する脆弱性が存在することが判明しました。

攻撃者はこの脆弱性を利用し、認証なく CPU ユニットが提供するファイルシステム（メモリカードまたは EM ファイルメモリ）へアクセスし、機微な情報を窃取できる可能性があります。

この脆弱性の影響を受ける製品、バージョン、対策、および軽減策・回避方法を以下に示します。弊社が推奨する軽減策・回避策を実施することで、本脆弱性の悪用リスクを最小限に抑えることができます

■対象製品

本脆弱性の影響を受ける製品の形式、およびバージョンは以下の通りです。

シリーズ	形式	対象バージョン
プログラマブルコントローラ SYSMAC CJ シリーズ	形 CJ2H-CPU6□-EIP 形 CJ2H-CPU6□	全てのバージョン
	形 CJ2M-CPU□□	全てのバージョン
	形 CJ1G-CPU□□P	全てのバージョン
SYSMAC CS シリーズ	形 CS1H-CPU□□H 形 CS1G-CPU□□H	全てのバージョン
	形 CS1D-CPU□□HA 形 CS1D-CPU□□H	全てのバージョン
	形 CS1D-CPU□□SA 形 CS1D-CPU□□S	全てのバージョン
	形 CS1D-CPU□□P	全てのバージョン

■脆弱性内容

プログラマブルコントローラ CS/CJ シリーズにおいて、「重要な機能に対する認証の欠如（CWE-306）」に関する脆弱性が存在することが判明しました。

■脆弱性により想定される脅威

攻撃者はこの脆弱性を利用し、認証なしで CPU ユニットが提供するファイルシステム（メモリカードまたは EM ファイルメモリ）へアクセスし、機微な情報を窃取できる可能性があります。

■CVSS スコア

重要な機能に対する認証の欠如（CWE-306）

CVE-2022-45794

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N 基本値 7.5

■軽減策・回避策

本脆弱性の悪用リスクを最小限に抑えるため、以下に示す軽減策を講じることを推奨します。

1.不正アクセスの防止

- 制御システムや装置のネットワーク接続を最小限に抑え、信頼できないデバイスからのアクセス禁止
- ファイアウォールの導入による IT ネットワークからの分離（未使通信ポートの遮断、通信ホストの制限、FINS ポート（9600）へのアクセスを制限）
- 制御システムや装置へのリモートアクセスが必要な場合、仮想プライベートネットワーク（VPN)の使用
- 強固なパスワードの採用と頻繁な変更
- 権限保有者のみを制御システムや装置へのアクセスを可能とする物理的統制の導入
- 制御システムや装置で USB メモリなど外部ストレージデバイスを使用する場合の事前ウイルススキャン
- 制御システムや装置へのリモートアクセス時の多要素認証の導入

さらに、以下に示す製品およびバージョンを使用されている場合、FINS 書込プロテクト機能を有効にすることで書き込みに対しても対策が可能です。

シリーズ	形式	対象バージョン	マニュアル
プログラマブルコントローラ SYSMAC CJ シリーズ	形 CJ2H-CPU6□-EIP 形 CJ2H-CPU6□	全てのバージョン	CJ シリーズ CJ2 CPU ユニット ユーザーズマニュアル ソフトウェア編（SBCA-350）「9-3-8 FINS プロテクト」を参照
	形 CJ2M-CPU□□	全てのバージョン	
	形 CJ1G-CPU□□P	ユニット Ver. 2.0 以降	CJ シリーズ ユーザーズマニュアル セットアップ編

			（ SBCA-312 ）「1-7-3 ネットワーク経由での、CPU ユニットに対する FINS 書込プロテクト機能」を参照
SYSMAC CS シリーズ	形 CS1H-CPU□□H 形 CS1G-CPU□□H	ユニット Ver. 2.0 以降	CS シリーズ CPU ユニット ユーザーズマニュアル セットアップ編 （ SBCA-301）「1-7-3 ネットワーク経由での、CPU ユニットに対する FINS 書込プロテクト機能」を参照
	形 CS1D-CPU□□SA 形 CS1D-CPU□□S	全てのバージョン	CS シリーズ CS1D デュプレックスシステム ユーザーズマニュアル セットアップ編 （ SBCA-318 ）「6-2-9 FINS プロテクトタブ（CPU 単独システムのみ）」を参照

2. アンチウィルス保護

   制御システムに接続するパソコンに最新の商用品質のウイルス対策ソフトの導入・保守

3. データ入出力の保護

   制御システムや装置への入出力データの意図せぬ改変に備えた、バックアップや範囲チェックなどの妥当性の確認

4. 紛失データの復元

   データ紛失対策としての定期的な設定データのバックアップと保守

■お問い合わせ先

当社営業または販売店にお問い合わせください。

国内お問い合わせ先：https://www.fa.omron.co.jp/sales/local/

海外お問い合わせ先：https://www.ia.omron.com/global_network/index.html

■更新履歴

2023/04/17 新規作成