プログラマブルコントローラ CS/CJ/CP シリーズ FINS プロトコルにおける インタラクション頻度の不適切な制御の脆弱性

公開日 2023 年 9 月 19 日
最終更新日 2023 年 11 月 13 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/CP シリーズ FINS プロトコルにおいて、インタラクション頻度の不適切な制御（CWE-799）の脆弱性が存在することが判明しました。攻撃者は当該脆弱性を用いてパスワードで保護されたメモリ領域の保護を解除し、当該コントローラ製品内の情報を不正に取得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、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。また、お客様に製品をより安心して利用いただくために、今回製品セキュリティ強化の対策バージョンを用意いたしました。各製品の対策バージョンの提供について本文の対策方法に示しますので、対策の実施をお願いいたします。

■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 CJ シリーズ	CJ2H-CPU□□(-EIP)	Ver.1.4 およびそれ以前
	CJ2M-CPU□□	Ver.2.0 およびそれ以前
	CJ1G-CPU□□P	Ver.4.0 およびそれ以前
プログラマブルコントローラ CS シリーズ	CS1H-CPU□□H CS1G-CPU□□H	Ver.4.0 およびそれ以前
	CS1D-CPU□□H CS1D-CPU□□P	Ver.1.3 およびそれ以前
	CS1D-CPU□□S	Ver2.0 およびそれ以前
プログラマブルコントローラ CP シリーズ	CP1E-E CP1E-N	Ver.1.2 およびそれ以前

対象製品バージョンの確認方法は、以下マニュアルを参照下さい。

- CJ シリーズ CJ2 CPU ユニット ユーザーズマニュアル ハードウェア編（SBCA-349）
- CJ 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-312）

・ 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）
・ 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）
・ CP シリーズ CP1E CPU ユニット ユーザーズマニュアル ソフトウェア編（SBCA-354）
上記マニュアルの「CPU ユニットのユニットバージョン」参照

■脆弱性内容
プログラマブルコントローラ CS/CJ/CP シリーズ FINS プロトコルにおいて、インタラクション頻度の不適切な制御（CWE-799）の脆弱性により、当該製品に不正にアクセスし、操作できる脆弱性が存在します。

■脆弱性により想定される脅威
攻撃者は、FINS プロトコルを介して複数の「メモリ領域の保護解除」呼び出しを高速に連続して行うことで、パスワードで保護されたメモリ領域の保護を解除し、当該コントローラ製品内の情報を不正に取得できる可能性があります。

■CVSS スコア
インタラクション頻度の不適切な制御（CWE-799）
CVE-2022-45790
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. 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
2. 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（未使用通信ポートの遮断、通信ホストの制限）
・ 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
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

■対策方法

各製品を対策バージョンに更新することで、本脆弱性の対策が可能です。

以下に各製品の対策バージョン、および対策バージョンの提供時期を示します。

シリーズ	形式	対策バージョン	対策バージョン提供時期
プログラマブルコントローラ CJ シリーズ	CJ2H-CPU□□(-EIP)	Ver.1.5 以降	2016 年提供済
	CJ2M-CPU□□	Ver.2.1 以降	
	CJ1G-CPU□□P	Ver.4.1 以降	
プログラマブルコントローラ CS シリーズ	CS1H-CPU□□H CS1G-CPU□□H	Ver.4.1 以降	
	CS1D-CPU□□H CS1D-CPU□□P	Ver.1.4 以降	
	CS1D-CPU□□S	Ver2.1 以降	
プログラマブルコントローラ CP シリーズ	CP1E-E CP1E-N	Ver.1.3 以降	

本脆弱性に対策する際は、対策後のバージョン品を購入いただくようお願いします。

購入方法については、当社営業にお問い合わせください。

■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

■謝辞

Dragos 社の Reid Wightman 氏から CISA を通じて本脆弱性が報告されました。

脆弱性を発見、報告いただいた Reid Wightman 氏に感謝いたします。

■更新履歴

2023/9/19　新規作成

2023/11/13　対策品の入手方法を修正