プログラマブルコントローラ CJ/CS/CP シリーズの

ユーザメモリ保護機能回避に関する脆弱性

公開日 2023 年 03 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 CJ/CS/CP シリーズにおいて、「不適切なアクセス制御（CWE-284）」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、ユーザメモリ（以下、UM）の保護機構を回避し、パスワードの無効化や新たなパスワードの上書きや、ユーザプログラムの実行用（オブジェクト）コードやファンクションブロック定義の上書きが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
SYSMAC CP シリーズ	形 CP2E-E□□D□-□ 形 CP2E-S□□D□-□ 形 CP2E-N□□D□-□	全てのバージョン

シリーズ	形式	対象バージョン
SYSMAC CP シリーズ	形 CP1H-X40D□-□ 形 CP1H-XA40D□-□ 形 CP1H-Y20DT-D	全てのバージョン
	形 CP1L-EL20D□-□ 形 CP1L-EM□□D□-□ 形 CP1L-L□□D□-□ 形 CP1L-M□□D□-□	全てのバージョン
	形 CP1E-E□□D□-□ 形 CP1E-NA□□D□-□	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 CJ/CS/CP シリーズにおいて、「不適切なアクセス制御（CWE-284）」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、UM の保護機構を回避し、ユーザメモリ（以下、UM）の保護機構を回避し、パスワードの無効化や新たなパスワードの上書きや、ユーザプログラムの実行用（オブジェクト）コードやファンクションブロック定義の上書きができる可能性があります。

■CVSS スコア

不適切なアクセス制御（CWE-284）

CVE-2023-0811

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H　基本値 9.1

■対策方法

以下に示す製品を使用されている場合、(1)または(2)の対策により、本脆弱性への対策が可能になります。

(1) UM 書き込みを設定するハードスイッチ（CPU ユニット前面のディップスイッチ）を有効にする

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 ハードウェア編（SBCA-349）「3-1 CPU ユニット」を参照
	形 CJ2M-CPU□□	全てのバージョン	

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 CJ1G-CPU□□P	全てのバージョン	CJ シリーズ ユーザーズマニュアル セットアップ編 （ SBCA-312 ）「6-1 ディップスイッチの設定」を参照
SYSMAC CS シリーズ	形 CS1H-CPU□□H 形 CS1G-CPU□□H	全てのバージョン	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）「6-1 ディップスイッチの設定」を参照
	形 CS1D-CPU□□HA 形 CS1D-CPU□□H	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）「2-4 CPU ユニット」を参照
	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	
SYSMAC CP シリーズ	形 CP1H-X40D□-□ 形 CP1H-XA40D□-□ 形 CP1H-Y20DT-D	全てのバージョン	CP シリーズ CP1H CPU ユニット ユーザーズマニュアル（SBCA-340）「6-6-2 書込プロテクト」を参照
	形 CP1L-EL20D□-□ 形 CP1L-EM□□D□-□	全てのバージョン	CP シリーズ CP1L-EL/EM CPU ユニット ユーザーズマニュアル（SBCA-406）「8-7-2 書込プロテクト」を参照
	形 CP1L-L□□D□-□ 形 CP1L-M□□D□-□	全てのバージョン	CP シリーズ CP1L CPU ユニット ユーザーズマニュアル（SBCA-345）「6-7-2 書込プロテクト」を参照

(2) 「パスワードによる読出プロテクト機能」を設定し、かつ「プログラムの上書き禁止(オプション)」を設定する

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	ユニット Ver. 2.0 以降
SYSMAC CS シリーズ	形 CS1H-CPU□□H 形 CS1G-CPU□□H	ユニット Ver. 2.0 以降
	形 CS1D-CPU□□SA 形 CS1D-CPU□□S	全てのバージョン
SYSMAC CP シリーズ	形 CP1H-X40D□-□ 形 CP1H-XA40D□-□ 形 CP1H-Y20DT-D	全てのバージョン
	形 CP1L-EL20D□-□ 形 CP1L-EM□□D□-□ 形 CP1L-L□□D□-□ 形 CP1L-M□□D□-□	全てのバージョン

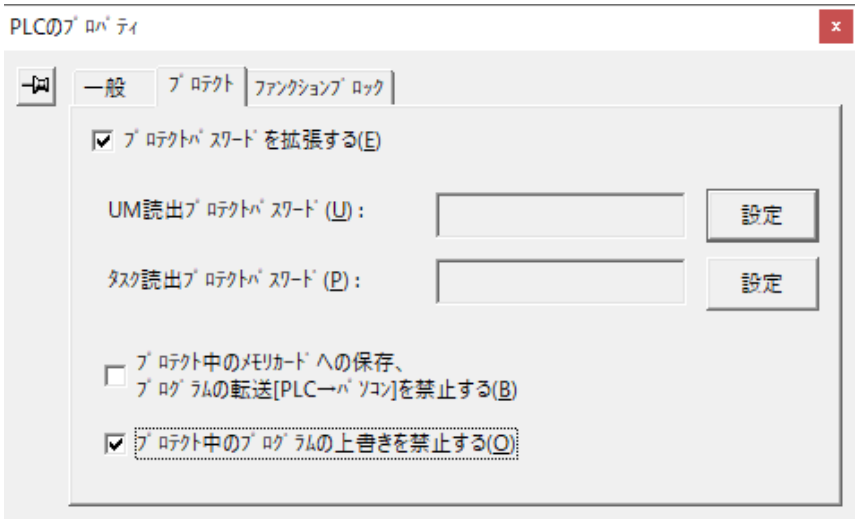
該当機能ついては、CX-Programmer Ver.9.□ オペレーションマニュアル（SBCA-337）「9-15 パスワードによる読出プロテクト」を参照してください。以下の手順で、設定します。

1. PLC のプロパティにて、パスワードを登録します。

   (1) 「プロテクト中のプログラムの上書きを禁止する」をチェックします。

   (2) UM 読出プロテクトパスワード右側の［設定］ボタンを選択します。
   拡張型読出プロテクト機能をサポートしている PLC および CX-Programmer9.6 以降を使用している場合は、UM 読出プロテクトパスワードの最大桁数を 16 桁に拡張が可能です。「プロテクトパスワードを拡張する」をチェックし、より強固なパスワードを設定することを推奨します。

拡張型読出プロテクト機能をサポートしている PLC の機種・バージョンは、「9－15 パスワードによる読出プロテクト ●プロテクトパスワードを拡張する（オプション）」を参照してください。



(3) ［プロテクト設定］ダイアログボックスにて、パスワードを入力し、［設定］ボタンを選択します。

(4) ［PLC のプロパティ］ダイアログボックスを閉じます。

2. オンライン接続して、PLC に読出プロテクトをかけます。

■軽減策・回避策

上記対策方法が適用できない場合は、以下の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

・ 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、(1)(2)の対策により、ネットワーク経由で攻撃者による攻撃のリスクを軽減できます。

(1) FINS 書込プロテクト機能を有効にする

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

シリーズ	形式	対象バージョン	マニュアル
SYSMAC CP シリーズ	形 CP1H-X40D□-□ 形 CP1H-XA40D□-□ 形 CP1H-Y20DT-D	全てのバージョン	CP シリーズ CP1H CPU ユニット ユーザーズマニュアル（SBCA-340）「6-6-2 書込プロテクト」を参照

(2) IP アドレスによるプロテクトをする

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 CP シリーズ	形 CP2E-N□□D□-□	全てのバージョン	CP シリーズ CP2E CPU ユニット ユーザーズマニュアル ソフトウェア編（SBCA-478）「15-4-4 PLC システム設定」を参照

さらに以下に示す対策を講じることを推奨します。

・ 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

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

■謝辞

Dragos 所属の Sam Hanson 氏から CISA(Cybersecurity & Infrastructure Security Agency)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 Sam Hanson 氏に感謝いたします。

■更新履歴

2023/03/13 新規作成