Sysmac Studio/CX-One 共通モジュールにおける バッファ開始位置にないポインタの開放の脆弱性

公開日 2024 年 4 月 22 日
オムロン株式会社

■概要

Sysmac Studio/CX-One 共通モジュールにおいて、バッファ開始位置にないポインタの開放 (CWE-761)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、任意のコードを実行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
CX-One	CX-One CXONE-AL□□D-V4	CX-One Ver.4.61.1 までの DVD でインストールされたもの、および、これに加えて CX-One オートアップデート(V4 向け_2024 年 01 月)までのいずれかのアップデートが適用されているもの
Sysmac Studio	SYSMAC-SE2□□□	Sysmac Studio Ver.1.56 までの DVD でインストールされたもの、および、これに加えて 2024 年 01 月 Sysmac Studio V1 オートアップデートまでのいずれかのアップデートが適用されているもの

対象製品バージョンの確認方法は、「別紙 製品バージョンの確認方法」を参照してください。

■脆弱性内容

Sysmac Studio/CX-One 共通モジュールにおいて、バッファ開始位置にないポインタの開放 (CWE-761)の脆弱性により、攻撃者は任意のコードを実行できる可能性があります。

■CVSS スコア

バッファ開始位置にないポインタの開放（CWE-761）

CVE-2024-31413

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H 基本値 7.8

■対策方法

Sysmac Studio/CX-One 共通モジュールに対して共通コンポーネントのアップデートを適用することで、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
CX-One	CX-One CXONE-AL□□D-V4	CX-One オートアップデート(V4 向け_2024 年 04 月)適用以降	2024 年 4 月 22 日
Sysmac Studio	SYSMAC-SE2□□□	2024 年 04 月 Sysmac Studio V1 オートアップデート適用以降（Ver.1.58 以降）	2024 年 4 月 22 日

対策バージョンの入手および更新方法については、以下リンク先にアクセスください。

CX-One バージョンアップ プログラム：サポートツール：オムロン（omron.co.jp)

Sysmac Studio バージョンアップ プログラム ダウンロード：サポートツール：オムロン（omron.co.jp)

■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

   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

■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

Michael Heinzl 氏から JPCERT/CC 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 Michael Heinzl 氏に感謝いたします。

■更新履歴

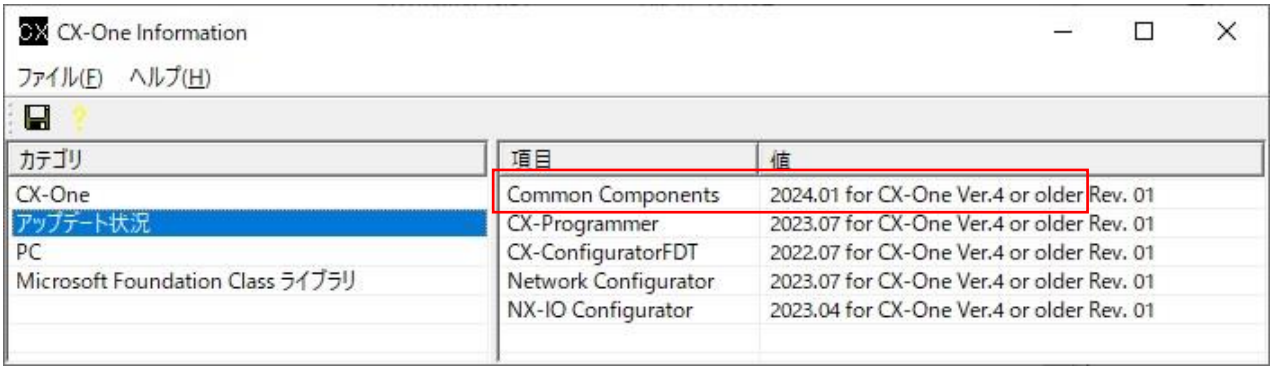
2024/4/22 新規作成

別紙　製品バージョンの確認方法

CX-One の確認方法

スタートメニュー – [Omron] – [CX-One] – [CX-One Information]から CX-One Information を起動し、「アップデート状況」から Common Components の値を確認してください。

※以下の例は CX-One オートアップデート(V4 向け_2024 年 01 月)がインストールされていることを示しています。



Sysmac Studio の確認方法

Sysmac Studio スタートページで「ライセンス」をクリックし、モジュールバージョンの値を確認してください。