# インバータ／サーボ用サポートツール CX-Drive における ヒープベースのバッファオーバーフローの脆弱性

公開日 2023 年 4 月 24 日
最終更新日 2023 年 8月 1 日
オムロン株式会社

■概要

インバータ／サーボ用サポートツール CX-Drive において、ヒープベースのバッファオーバーフロー（CWE-122）の脆弱性が存在することが判明しました。ローカルの攻撃者がこの問題を悪用して、情報を漏えいさせ、影響を受ける CX-Drive のインストールで任意のコードを実行する可能性があります。

この脆弱性を悪用するには、ユーザーの操作が必要となり、ユーザーが悪質な SDD ファイルを開くことが攻撃者にとっての必要条件となります。

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。

■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-Drive | 全形式 | 全てのバージョン |

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。

・ CX-Drive オペレーションユーザーズマニュアル（SBCE-375）

■CVSS スコア

ヒープベースのバッファオーバーフロー（CWE-122）
CVE-2023-27385
CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H 基本値 7.8

■軽減策 ・回避方法

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・回避方法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
   ・ 不審なプロジェクトファイルの実行をしない

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

5. 新しいソフトウェアツール及びコントローラの採用

・オートメーションソフトウェア Sysmac Studio
・コントローラ NJ/NX/NY シリーズ

■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、報告いただいたい Michael Heinzl 氏に感謝いたします。

■更新履歴

2023/4/24　新規作成
2023/8/1　対象製品のバージョンを追加