マシンオートメーションコントローラ NJ/NX の
データ真正性の検証が不十分な脆弱性

公開日 2024 年 5 月 27 日
オムロン株式会社

■概要

マシンオートメーションコントローラ NJ/NX シリーズにおいて、データ真正性の検証が不十分（CWE-345）な脆弱性が存在することが判明しました。当該脆弱性により、当該コントローラ製品は製品内のユーザプログラムが改ざんされたことを検知できない可能性があります。

この脆弱性の影響を受ける製品、バージョン、対策方法、および軽減策・回避方法を以下に示します。弊社が推奨する対策方法、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。

- マシンオートメーションコントローラ NJ シリーズ CPU ユニット 全バージョン
- マシンオートメーションコントローラ NX シリーズ CPU ユニット 全バージョン

■脆弱性内容

マシンオートメーションコントローラ NJ/NX シリーズにおいて、データ真正性の検証が不十分（CWE-345）な脆弱性により、当該コントローラ製品は製品内のユーザプログラムが改ざんされたことを検知できない可能性があります。

■CVSS スコア

データ真正性の検証が不十分（CWE-345）
CVE-2024-33687
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N 基本値 4.8

■対策方法

以下の対策により、本脆弱性への対策が可能です。

1. ユーザプログラム復元情報無し転送機能の使用
   通常は、Sysmac Studio から CPU ユニットにユーザプログラムを転送するときに、その復元のための情報も転送しています。本機能は、このときに、復元のための情報を転送しないため、ユーザプログラムを改ざんすることができなくなります。使用方法は以下のマニュアルの 「ユーザプログラム復元情報無し転送機能」を参照ください。
   - NJ/NX シリーズ CPU ユニット ユーザーズマニュアルソフトウェア編（SBCA-467）

■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

Microsoft 社の CPS Research Team の Tamir Ariel 氏から報告されました。

脆弱性を発見、報告いただいた Tamir Ariel 氏に感謝いたします。

■更新履歴

2024/5/27 新規作成