

マシンオートメーションコントローラ NJ/NX シリーズの 通信機能における認証回避の脆弱性

公開日 2022 年 7 月 1 日
最終更新日 2022 年 10 月 11 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 シリーズとオートメーションソフトウェア Sysmac Studio およびプログラマブルターミナル NA シリーズとの通信機能において、ハードコードされた認証情報の使用（CWE-798）および、Capture-replay による認証回避（CWE-294）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通信接続時の認証を回避し、当該コントローラ製品に不正にアクセス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
マシンオートメーションコントローラ NX7 シリーズ	全形式	V1.28 以下
マシンオートメーションコントローラ NX1 シリーズ	全形式	V1.48 以下
マシンオートメーションコントローラ NJ シリーズ	全形式	V1.48 以下
オートメーションソフトウェア Sysmac Studio	全形式	V1.49 以下
プログラマブルターミナル NA シリーズ	形 NA5-15W 形 NA5-12W 形 NA5-9W 形 NA5-7W	Runtime V1.15 以下

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。

- ・ NX シリーズ CPU ユニット ユーザーズマニュアル ハードウェア編 (SBCA-418)
- ・ NX シリーズ 形 NX102 CPU ユニット ユーザーズマニュアル ハードウェア編 (SBCA-462)
- ・ NX シリーズ 形 NX1P2 CPU ユニット ユーザーズマニュアル ハードウェア編 (SBCA-448)
- ・ NJ シリーズ CPU ユニット ユーザーズマニュアル ハードウェア編 (SBCA-466)
上記マニュアルの「バージョンの確認方法」参照
- ・ NA シリーズ ユーザーズマニュアル ハードウェア編 (SBSA-545)
- ・ NA シリーズ ユーザーズマニュアル ハードウェア (-V1) 編 (SBSA-558)
上記マニュアルの「システムメニューの概要」参照(システムメニュー画面左下で Runtime バージョン確認可能)
- ・ Sysmac Studio Version 1 オペレーションマニュアル (SBCA-470) の「ライセンスの表示と登録」参照

■脆弱性内容

マシンオートメーションコントローラ NJ/NX シリーズとオートメーションソフトウェア Sysmac Studio およびプログラマブルターミナル NA シリーズの通信機能において、ハードコードされた認証情報の使用 (CWE-798) および、Capture-replay による認証回避 (CWE-294) の脆弱性により、当該製品を不正にログイン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

攻撃者は当該脆弱性を用いて通信接続時の認証を回避し、当該コントローラに不正にログインし操作できる可能性があります。

■CVSS スコア

(1) ハードコートされた認証情報の使用(CWE-798)

CVE-2022-34151

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H 基本値 9.4

(2) Capture-replay による認証回避(CWE-294)

CVE-2022-33208

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H 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. アンチウイルス保護

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
マシンオートメーションコントローラ NX7 シリーズ	全形式	V1.29 以上	2022 年 10 月 11 日
マシンオートメーションコントローラ NX1 シリーズ	全形式	V1.50 以上	2022 年 10 月 11 日
マシンオートメーションコントローラ NJ シリーズ	形 NJ501-1300 形 NJ501-1400 形 NJ501-1500	V1.49 以上	2022 年 7 月 1 日
	上記以外の形式	V1.50 以上	2022 年 10 月 11 日
オートメーションソフトウェア Sysmac Studio	全形式	V1.50 以上	2022 年 7 月 1 日
プログラマブルターミナル NA シリーズ	形 NA5-15W 形 NA5-12W 形 NA5-9W 形 NA5-7W	Runtime V1.16 以上	2022 年 7 月 1 日

製品の対策バージョンファームウェアの入手および更新方法については、当社営業にお問い合わせ下さい。また、Sysmac Studio は、以下リンク先を参考に、ソフトウェアを最新に更新してください。

https://www.fa.omron.co.jp/product/tool/install_manual/index.html

コントローラの以下セキュリティ機能を用いて対策を講じることを推奨します。機能の詳細、設定方法については、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) 「8-5 セキュリティ機能」を参照してください。

- ・セキュア通信機能を用いて、Sysmac Studio や NA シリーズとコントローラとの通信データを暗号化することで、第三者によるデータの盗聴や改ざんを防止できます。
- ・Packet Filter 機能を用いて、内蔵 EtherNet/IP ポートの受信処理にて IP パケットをフィルタリングすることにより、外部からの不正なアクセスに対して制限をかけることができます。
- ・ユーザ認証機能を用いて、ツールオンライン時に個々のユーザに対して認証を行い、ユーザの権限に応じた操作のみ可能とすることで、不正なアクセスを防止することができます。

■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

■その他

本脆弱性および対策は、米国 Cybersecurity & Infrastructure Security Agency (CISA) にて以下報告された脆弱性攻撃ツールが用いる脆弱性、および対策に該当します。

APT Cyber Tools Targeting ICS/SCADA Devices

<https://www.cisa.gov/uscert/ncas/alerts/aa22-103a>

■更新履歴

2022/7/1 新規作成

2022/10/11 以下 2 点を修正

- (1) 「対策方法」の対策バージョン提供時期を更新
- (2) 脆弱性評価の見直しに伴い、以下を変更
 - ・ CVE-2022-34151 の CVSS スコア
(変更前) CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:H 基本値 7.7
(変更後) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H 基本値 9.4
 - ・ CVE-2022-33208 の CVSS スコア
(変更前) CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:H/A:H 基本値 6.2
(変更後) CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H 基本値 7.5