複数のオムロン製品に実装されている

FINS プロトコルにおける既知の問題について

公開日 2023 年 4 月 17 日
最終更新日 2023 年 9 月 19 日
オムロン株式会社

■概要

FINS(Factory Interface Network Service)は、オムロン社製品で構成された FA ネットワークで使用されるメッセージ通信のプロトコルです。オムロン社のプログラマブルコントローラ(PLC)には、FINS プロトコルの仕様に起因する既知の問題が報告されています。

■影響を受ける代表的な機器

- プログラマブルコントローラ CS シリーズ CPU ユニット 全バージョン
- プログラマブルコントローラ CJ シリーズ CPU ユニット 全バージョン
- プログラマブルコントローラ CP 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 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 NX1P 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 NX102 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 NX7 データベース接続 CPU ユニット 全バージョン

■詳細情報

FINS プロトコルは、オムロン社製の PLC や PC ソフトウェアなど、FA(Factory Automation)ネットワークの制御用途として開発された、軽量かつシンプルな通信プロトコルです。FINS プロトコルは、コマンド・レスポンス方式のメッセージで通信を行い、FA 制御システムのモニタ・操作・設定をすることができます。

FINS コマンドには、各種のコマンドが用意されおり、大別して、以下の種類があります。

・I/O メモリエリアの読み出し/書き込み
・パラメータエリアの読み出し/書き込み
・プログラムエリアの読み出し/書き込み
・動作モード変更
・機器構成の読み出し
・CPU ユニットのステータスの読み出し
・時間情報のアクセス

・メッセージの読み出し/解除
・アクセス権の獲得・開放
・異常履歴の読み出しなど
・ファイル操作
・強制セット/リセット
これらの情報は、マニュアル等で公開されており、仕様が開示されています。機種により、サポートする FINS コマンドは異なります。

FINS コマンドのメッセージは、「FINS ヘッダ」「FINS コマンドコード」「パラメータ」の 3 つから構成されています。FINS コマンドメッセージを受信した制御機器/ソフトウェアは、その「FINS コマンドコード」に対応する処理を実行し、その処理結果を FINS レスポンスメッセージとして、「FINS ヘッダ」にある送信元へ返信します。

FINS のプロトコル設計当時、FA ネットワークは工場やライン・装置に閉じたローカルネットワークであることを前提としていました。そのため、FA ネットワークがオープンネットワーク化した現在では、FINS 仕様に対して、いくつかの脆弱性が指摘されています。

1. 平文通信
FINS プロトコル仕様では、暗号化通信を規定していません。よって、通信経路上の FINS メッセージは平文で送受信されるため、容易に傍受することができます。また、FINS メッセージの改ざんを検知することが出来ません。

- 機微な情報の平文通信（CWE-319）
- データの信頼性についての不十分な検証（CWE-345）

2. 認証不要
FINS プロトコル仕様では、認証処理は規定していません。よって、悪意ある通信相手からの攻撃であることを識別することはできません

- なりすましによる認証回避（CWE-290）
- Capture-replay 攻撃による認証回避（CWE-294）
- 重要な機能に対する認証の欠如（CWE-306）
- データの信頼性についての不十分な検証（CWE-345）
- サービス運用妨害（DoS）の脆弱性（CWE-400）
- 外部からの操作制限不備（CWE-412）
- インタラクション頻度の不適切な制御（CWE-799）

これらの脆弱性は、FINS プロトコルの仕様に起因しますが、仕様改訂の予定はありません。

■想定される影響

第三者によって、通信内容が搾取されることや、不正な制御コマンド実行、制御システム情報への不正アクセス等が行われる可能性があります。

■対策方法

本脆弱性の悪用リスクを最小限に抑えるため、以下に示す軽減策を講じることを推奨します。

1.FINS を使用しない(FINS を無効化する)

FINS を使用していない FA ネットワークの場合、以下の機種では FINS を無効化することで、FINS 仕様に起因する脆弱性を防ぐことができます。

- 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 (Ver.1.49 以降)
- マシンオートメーションコントローラ NX1P シリーズ CPU ユニット (Ver.1.50 以降)
- マシンオートメーションコントローラ NX102 シリーズ CPU ユニット (Ver.1.50 以降)
- マシンオートメーションコントローラ NX7 データベース接続 CPU ユニット (Ver.1.29 以降)

2.不正アクセスの防止

次に示す回避策を適用することで、脆弱性の影響を軽減することが可能です。

- アクセス元 IP アドレスを制限する
- 許可されていないネットワークアセスを制限する
- FINS 書込プロテクト機能を有効にする
- PLC 保護パスワードを使用することで、書き込み権限を制約する。
- PLC 上のハードウェア DIP スイッチを使用することで、PLC プログラム変更を禁止する (プログラマブルコントローラ CS/CJ シリーズ CPU ユニット、CP シリーズ CP1H/CP1L CPU ユニットの場合)

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（未使用通信ポートの遮断、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

3.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。

4.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。

5.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。

また、既知の問題について、以下に記載されていますので、ご参照の上、対策をご検討ください。

・JVNVU#91000130

オムロン製 PLC CJ シリーズにおけるサービス運用妨害 (DoS) の脆弱性

https://jvn.jp/vu/JVNVU91000130/

・JVNVU#91952379

複数のオムロン製 PLC における複数の脆弱性

https://jvn.jp/vu/JVNVU91952379/

・JVNVU#97111518

オムロン製 SYSMAC CS/CJ/CP シリーズおよび NJ/NX シリーズにおける複数の脆弱性

https://jvn.jp/vu/JVNVU97111518/

既知の問題として報告されている機種以外において、本書で説明された FINS の仕様に起因する脆弱性である場合は、既知の問題として取り扱い致します。

■関連文書

・弊社 PLC に対する外部機関からの脆弱性指摘について

https://www.omron-cxone.com/security/2019-12-06_PLC_JP.pdf

・CS/CJ/CP/NSJ シリーズ 通信コマンド リファレンスマニュアル (SBCA-304)

・NX シリーズ CPU ユニット ユーザーズマニュアル FINS 機能編（SBCD-375）

■更新履歴

日付	履歴
2023 年 4 月 17 日	初版発行
2023 年 9 月 19 日	誤記修正