# 關於多款歐姆龍產品安裝的FINS協定中存在的已知問題

發佈日期：2023年4月17日
更新日期：2023年9月19日
台灣歐姆龍股份有限公司

■概要

歐姆龍一直致力於在工業自動化領域為客戶提供安全、可靠、高品質的產品與解決方案，這是我們立足行業，持續助推客戶業務增長，為客戶創造價值的根基。
FINS（Factory Interface Network Service，工廠介面網路服務），是用於由歐姆龍公司產品構成的FA網路中的資訊通信協定。此次將歐姆龍公司的可程式設計控制器（PLC）中存在由FINS協議引發的已知問題、以及相應對策方法進行彙總聯絡。

■受影響的代表性設備

・可編程控制器 CS系列 CPU單元 全部版本
・可編程控制器 CJ系列 CPU單元 全部版本
・可編程控制器 CP系列 CPU單元 全部版本
・機械自動化控制器 NJ系列 CPU單元 全部版本
・機械自動化控制器 NX1P系列 CPU單元 全部版本
・機械自動化控制器 NX102系列 CPU單元 全部版本
・機械自動化控制器 NX7資料庫連接CPU單元 全部版本

■詳細資訊

FINS協定是一種輕量、簡單的通信協定，用於控制歐姆龍公司生產的PLC和PC軟體等FA（Factory Automation，工廠自動化）網路。 FINS協議能夠進行指令和回應式資訊通信，從而監視、操作或設定FA控制系統。

FINS指令種類繁多，大致可分為以下幾類。

・I/O記憶體區的讀取/寫入
・參數區的讀取/寫入
・程式區的讀取/寫入
・運行模式變更
・設備構成的讀取
・CPU單元狀態的讀取
・時間資訊的存取

・訊息的讀取/解除
・取得/釋放存取權限
・異常歷史的讀取等
・檔案操作
・強制設定/重置
這些資訊已在操作手冊等文件中公開，且規格已揭示。根據不同的機型，所支援的FINS指令也有所不同。

FINS指令訊息由「FINS標頭」、「FINS指令代碼」以及「參數」這三個部分構成。當控制設備或軟體接收到FINS指令訊息後，會執行與「FINS指令代碼」相對應的處理，並將處理結果作為FINS回應訊息，回傳給「FINS標頭」中所指定的發送來源。

當初設計FINS協定時，是基於FA網路是以工廠、生產線和設備內部的封閉化本地網路為前提。因此，在FA網路已成為開放網路的現在，對於FINS協議規格，被指出存在一些漏洞。

1.明文通信
FINS協議規格未對加密通信。 因此，通信線路中的FINS消息以明文形式收發，易遭監聽。 此外，也無法檢測FINS資訊是否被篡改。

・機密資訊的明文通信（CWE-319）
・未充分驗證數據可靠性（CWE-345）

2.無需認證
FINS協議規格未對認證處理進行規定。 因此無法識別是否遭受惡意通信對象攻擊。

・通過欺騙迴避認證（CWE-290）
・通過捕捉-重播攻擊迴避認證（CWE-294）
・缺失對關鍵功能的認證（CWE-306）
・未充分驗證數據可靠性（CWE-345）
・干擾服務運行（DoS）的漏洞（CWE-400）
・對來自外部的操作的限制不完備（CWE-412）
・交互頻率控制不當（CWE-799）

這些漏洞是由FINS協議規格所引起的，但目前尚無修訂規格的計劃。

■預期影響

第三方可能會監聽通信內容，執行非法控制指令或未經授權而訪問控制系統資訊。

■對策方法

為將該漏洞的惡意利用風險降至最低，建議採取以下減輕措施。

1. 停用FINS（不使用FINS）

如果FA網路不使用FINS，以下機型可以透過停用FINS來防止FINS協定規範所帶來的漏洞：

- 機械自動化控制器 NJ系列 CPU單元（版本1.49以上）
- 機械自動化控制器 NX1P系列 CPU單元（版本1.50以上）
- 機械自動化控制器 NX102系列 CPU單元（版本1.50以上）
- 機械自動化控制器 NX7資料庫連接CPU單元（版本1.29以上）

2. 防止未經授權存取

透過採取以下措施，可以減輕漏洞帶來的影響：

- 限制存取來源的IP位址
- 限制未經授權的網路存取
- 啟用FINS寫入保護功能
- 使用PLC保護密碼，限制寫入權限
- 使用PLC上的硬體DIP開關，禁止PLC程式變更（適用於可編程控制器CS/CJ系列CPU單元及CP系列CP1H/CP1L CPU單元）

此外，建議採取以下對策來進一步增強安全性：

- 將控制系統與設備的網路連接減至最小，禁止來自不可信設備的存取
- 透過引入防火牆將IT網路隔離（關閉未使用的通訊埠、限制通訊主機，並限制對FINS埠（9600）的存取）
- 如果控制系統或設備需要遠端存取，應使用虛擬私人網路（VPN）
- 採用強密碼並頻繁更換
- 只允許具備權限者存取控制系統或設備，並實施物理控制
- 使用USB記憶體等外部存儲設備時，必須事先進行病毒掃描
- 對控制系統或設備的遠端存取，應啟用多因素身份驗證

3. 防病毒保護

在連接控制系統的電腦上安裝和維護最新的商業級防病毒軟體。

4. 數據輸入輸出的保護
為防範控制系統或設備的輸入輸出數據意外更改，應進行備份和範圍檢查等合理性確認。

5. 數據丟失的恢復
定期備份和維護設定數據，以應對數據丟失的問題。

此外，關於已知問題，請參考以下資訊並考慮相應對策：
・JVNVU#91000130
歐姆龍製PLC CJ系列中的服務運行干擾（DoS）漏洞
https://jvn.jp/vu/JVNVU91000130/

・JVNVU#91952379
多款歐姆龍製PLC中的多個漏洞
https://jvn.jp/vu/JVNVU91952379/

・JVNVU#97111518
歐姆龍製SYSMAC CS/CJ/CP系列及NJ/NX系列中的多個漏洞
https://jvn.jp/vu/JVNVU97111518/

如果其他機型存在與本文件中說明的FINS規範有關的漏洞，將視為已知問題處理。

■相關文件

・我們公司對PLC的外部機構漏洞指摘的回應
https://www.omron-cxone.com/security/2019-12-06_PLC_EN.pdf

・CS/CJ/CP/NSJ系列通訊指令參考手冊（SBCA-304）

・NX系列CPU單元用戶手冊 FINS功能篇（SBCD-375）

■更新記錄
2023年4月17日 建立
2023年9月19日 誤記修正