About Known Issues in the FINS Protocol Implemented in Omron Products

Release date: April 17, 2023
Last modified on September 19, 2023
Omron Corporation

■ Overview

FINS (Factory Interface Network Service) is a message communications protocol used in factory automation (FA) networks built with Omron products. Known issues due to FINS protocol specifications have been reported on the Omron Programmable Logic Controller (PLC).

■ Main products affected

- Programmable Controller CS-series CPU Units, all versions
- Programmable Controller CJ-series CPU Units, all versions
- Programmable Controller CP-series CPU Units, all versions
- Machine Automation Controller NJ-series CPU Units, all versions
- Machine Automation Controller NX1P-series CPU Units, all versions
- Machine Automation Controller NX102-series CPU Units, all versions
- Machine Automation Controller NX7 Database Connection CPU Units, all versions

■ Detailed information

The FINS protocol is a lightweight and simple communications protocol developed for controlling FA networks consisting of Omron PLCs and PC software. The FINS protocol can be used for command-response message communications and enables monitoring, operation, and setting of the FA control system.

Various FINS commands are available, which can be classified into the following types.

・Reading and writing values of I/O memory area
・Reading and writing values in parameter area
・Reading and writing values in program area
・Changing the operating mode
・Reading device configuration
・Reading CPU Unit status
・Access to time information

・Reading messages and clearing them
・Acquiring and releasing access right
・Reading error logs, etc.
・Operating files
・Forced set/reset

This information is published in manuals, etc., and the specifications are disclosed. Supported FINS command differs depending on the product model.

The FINS command message consists of three elements: "FINS header", "FINS command code" and "parameter". The control device/software that receives the FINS command message processes the FINS command code and returns the processing result as a FINS response message to the source of the command in the FINS header.

When the FINS protocol was developed, it was assumed that the FA network would be a local network closed within factories, lines, and equipment, or devices. Now that FA networks have become open networks, some vulnerabilities have been pointed out in the FINS specifications.

1. Cleartext communications

The FINS protocol does not support encrypted communications in its specifications. Since FINS messages are sent and received without being encrypted, they can be intercepted. Also, it is difficult to detect falsification of FINS messages.

- Cleartext Transmission of Sensitive Information (CWE-319)
- Insufficient Verification of Data Authenticity (CWE-345)

2. No verification or authentication is required

The FINS protocol does not support the authentication process in its specifications. Therefore, an attack from a malicious communication device cannot be detected.

- Authentication Bypass by Spoofing (CWE-290)
- Authentication Bypass by Capture-replay (CWE-294)
- Missing Authentication for Critical Function (CWE-306)
- Insufficient Verification of Data Authenticity (CWE-345)
- Uncontrolled Resource Consumption (CWE-400)
- Unrestricted Externally Accessible Lock (CWE-412)
- Improper Control of Interaction Frequency (CWE-799)

These vulnerabilities are due to the specifications of the FINS protocol, but there are no plans to revise the specifications.

■ Expected threats

A third party may exploit the content of communications or execute unauthorized command or malicious access to control system.

■ Countermeasures

To minimize the risk of exploitation of this vulnerability, we recommend the following mitigation measures.

1. Do not use FINS (disable FINS)

For FA networks that do not use FINS, vulnerabilities caused by the FINS specifications can be prevented by disabling FINS on the following models.

- Machine Automation Controller NJ-series CPU Units (Ver.1.49 or higher)
- Machine Automation Controller NX1P-series CPU Units (Ver.1.50 or higher)
- Machine Automation Controller NX102-series CPU Units (Ver.1.50 or higher)
- Machine Automation Controller NX7 Database Connection CPU Units (Ver.1.29 or higher)

2. Security measures to prevent unauthorized access

Applying the following workarounds can mitigate the effects of the vulnerability.

・Restrict IP Address of access source

・Restrict unauthorized access to networks

・Enable the FINS write protection function

・Restrict write permissions by using a password for write-protecting the PLC

・Prohibit PLC programs changes by using hardware DIP switches on the PLC (Programmable Controller CS/CJ -series CPU Units, CP-series CP1H/CP1L CPU Units)

In addition, it is recommended to take the following measures.

・ Reduce connections to control systems and equipment via networks to prevent access from untrusted devices.

・ Separate control systems from the IT network by introducing a firewall (blocking unused communication ports, limiting communication hosts, limiting access to the FINS port (9600))

・ Use a virtual private network (VPN) for remote access to control systems and equipment.

・ Set strong passwords and change them frequently.

・ Install physical controls so that only authorized personnel can access control systems and equipment.

・ Scan virus to ensure safety of USB memory or other external storages before connecting them to control systems and equipment.

・ Adopt multifactor authentication to devices with remote access to control systems and equipment.

3. Antivirus protection

Install the latest commercial-quality antivirus software on computers connected to control systems and keep it up to date.

4. Data input and output protection

Validate backups and check ranges to cope with unintentional modification of input/output data to control systems and equipment.

5. Data recovery

Regularly backup configuration data and maintain it in case of data loss.

In addition, the known issues are described below, so please refer to them and consider implementing countermeasures.

・ICS Advisory (ICSA-20-063-03), Omron PLC CJ Series
https://www.us-cert.gov/ics/advisories/icsa-20-063-03

・ICS Advisory (ICSA-19-346-02), Omron PLC CJ and CS Series
https://www.us-cert.gov/ics/advisories/icsa-19-346-02

・ICS Advisory (ICSA-22-179-02), Omron SYSMAC CS/CJ/CP Series and NJ/NX Series
https://www.cisa.gov/news-events/ics-advisories/icsa-22-179-02

For models other than those reported for known issues, if the vulnerability is caused by the FINS specifications described in this document, it will be treated as a known issue.

■ Related documents

・Vulnerabilities in Omron PLCs
https://www.omron-cxone.com/security/2019-12-06_PLC_EN.pdf

・CS/CJ/CP/NSJ-series Communications Commands Reference Manual (Cat. No. W342)

・NX-series CPU Unit FINS Function User’s Manual (Cat. No. W596)

■ Revision history

Date	History
April 17, 2023	First edition
September 19, 2023	Clerical Corrections