# Improper Control of Interaction Frequency in FINS protocol between the CS/CJ/CP-series Programable Controllers

Release date: September 19, 2023
Last modified on November 13, 2023
OMRON Corporation

## ■Overview

Improper Control of Interaction Frequency (CWE-799) vulnerabilities exist in the FINS protocol between the CS/CJ/CP-series Programable Controllers. An attacker may use these vulnerabilities to unprotect password-protected memory areas and gain information in the controller product unauthorizedly.

The products and versions affected by these vulnerabilities, mitigation and protection measures are shown below. Make sure to implement these recommended mitigations and protections to minimize the risk of exploitation of these vulnerabilities. Moreover, to ensure that customers use our products with confidence, the security enhanced countermeasure version of each product has been prepared. Please check countermeasures shown below in this document and implement appropriate countermeasures.

## ■Affected products

Affected products and versions are below.

| Product series | Model | Version |
|---|---|---|
| CJ-series Programable Controller | CJ2H-CPU[][](-EIP) | Ver.1.4 or lower |
| | CJ2M-CPU[][] | Ver.2.0 or lower |
| | CJ1G-CPU[][]P | Ver.4.0 or lower |
| CS-series Programable Controller | CS1H-CPU[][]H<br>CS1G-CPU[][]H | Ver.4.0 or lower |
| | CS1D-CPU[][]H<br>CS1D-CPU[][]P | Ver.1.3 or lower |
| | CS1D-CPU[][]S | Ver.2.0 or lower |
| CP-series | CP1E-E | Ver.1.2 or lower |

| | | |
|---|---|---|
| Programable Controller | CP1E-N | |

Refer to the following manuals for how to check the target product version.

- CJ-series CJ2 CPU Unit User's Manual (Hardware) (W472)
- CJ-series Programable Controllers Operation Manual (W393)
- CS-series Programable Controllers Operation Manual (W339)
- CS-series CS1D Duplex system Operation Manual (W405)
- CP-series CP1E CPU Unit User's Manual (Hardware) (W479)

Refer to "Checking Versions" section in the above manuals.

■Description

Due to the Improper Control of Interaction Frequency (CWE-799) vulnerabilities which exist in the FINS protocol between the CS/CJ/CP-series Programable Controllers, the products may be gain unauthorized access.

■Potential threats and impacts

An attacker may use the vulnerabilities to unprotect password-protected memory areas and gain information in the controller product unauthorizedly.

■CVSS Scores

Improper Control of Interaction Frequency (CWE-799)
CVE-2022-45790
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N Base Score 7.5

■Mitigations and Protections

OMRON recommends that customers take the following mitigation measures to minimize the risk of exploitation of these vulnerabilities.

1. Anti-virus protection

   Protect any PC with access to the control system against malware and ensure installation and maintenance of up-to-date commercial grade anti-virus software protection.

2. Security measures to prevent unauthorized access

   - Minimize connection of control systems and equipment to open networks, so that untrusted devices will be unable to access them.
   - Implement firewalls (by shutting down unused communications ports, limiting communications hosts) and isolate them from the IT network.
   - Use a virtual private network (VPN) for remote access to control systems and equipment.

- Use 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 any USB drives or similar devices before connecting them to systems and devices.
- Enforce multifactor authentication to all devices with remote access to control systems and equipment whenever possible.

3. Data input and output protection

Validation processing such as backup and range check to cope with unintentional modification of input/output data to control systems and devices.

4. Data recovery

Periodical data backup and maintenance to prepare for data loss.

■Countermeasures

The countermeasures against the vulnerabilities can be implemented by updating each product to the countermeasure version. The countermeasure version and respective release date for each product is shown in the table below.

| Product series | Model | Version | Release date |
|---|---|---|---|
| CJ-series Programable Controller | CJ2H-CPU[][](-EIP) | Ver.1.5 or higher | Released in 2016 |
| | CJ2M-CPU[][] | Ver.2.1 or higher | |
| | CJ1G-CPU[][]P | Ver.4.1 or higher | |
| CS-series Programable Controller | CS1H-CPU[][]H<br>CS1G-CPU[][]H | Ver.4.1 or higher | |
| | CS1D-CPU[][]H<br>CS1D-CPU[][]P | Ver.1.4 or higher | |
| | CS1D-CPU[][]S | Ver2.1 or higher | |
| CP-series Programable Controller | CP1E-E<br>CP1E-N | Ver.1.3 or higher | |

Please purchase the countermeasure version of the product to take measures against this vulnerability. Please contact our sales office or distributors for purchasing instructions.

■Contact information

Please contact our sales office or distributors.

https://www.ia.omron.com/global_network/index.html

■Acknowledgments

Reid Wightman of Dragos reported this vulnerability through CISA.

Thanks to Reid Wightman for finding and reporting it.

■Update history

- September 19, 2023: New Release
- November 13, 2023: Corrected method of obtaining countermeasures