Missing Authentication Vulnerabilities related to file system of CS/CJ-series Programmable Controllers

Release date: April 17, 2023
OMRON Corporation

■Overview

Missing Authentication for Critical Function (CWE-306) vulnerabilities exist in the CS/CJ-series Programmable Controllers.

An attacker may use these vulnerabilities to access to the file system (Memory card or EM file memory) provided by the CPU Unit without authentication and obtain available sensitive information.

.

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.

■Affected products

Affected products and versions are below.

Product series	Model	Version
Programmable Controller SYSMAC CJ-series	CJ2H-CPU6□-EIP CJ2H-CPU6□	All versions
	CJ2M-CPU□□	All versions
	CJ1G-CPU□□P	All versions
SYSMAC CS-series	CS1H-CPU□□H CS1G-CPU□□H	All versions
	CS1D-CPU□□HA CS1D-CPU□□H	All versions
	CS1D-CPU□□SA CS1D-CPU□□S	All versions
	CS1D-CPU□□P	All versions

■Description

Insufficient Verification of Data Authenticity (CWE-345) vulnerabilities exist in the CS/CJ-series Programmable Controllers.

■Potential threats and impacts

An attacker may use these vulnerabilities to access to the file system (Memory card or EM file memory) provided by the CPU Unit without authentication and obtain available sensitive information.

■CVSS Scores

Missing Authentication for Critical Function (CWE-306)
CVE-2022-45794
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. Security measures to prevent unauthorized access
   - If the following products and versions are used, the risk for which an attacker will access to the file system (Memory card or EM file memory) provided by the CPU Unit without authentication via a network can be reduced by taking following measure 1).

1) Enable the FINS write protection function.

Product series	Model	Version	Manual
Programmable Controller SYSMAC CJ-series	CJ2H-CPU6□-EIP CJ2H-CPU6□	All versions	Refer to 9-3-8 FINS Protection in the CJ-series CJ2 CPU Unit Software User's Manual (Cat. No. W473).
	CJ2M-CPU□□	All versions	
	CJ1G-CPU□□P	Unit version 2.0 or lower	Refer to 1-7-3 Write Protection from FINS Commands Sent to CPU Units via

			Networks in the CJ-series Programmable Controllers Operation Manual (Cat. No. W393).
SYSMAC CS-series	CS1H-CPU□□H CS1G-CPU□□H	Unit version 2.0 or lower	Refer to 1-7-3 Write Protection from FINS Commands Sent to CPU Units via Networks in the CS-series Programmable Controllers Operation Manual （Cat. No. W339）.
	CS1D-CPU□□SA CS1D-CPU□□S	All versions	Refer to 6-2-9 FINS Protection Tab Page (Single CPU Systems Only) in the CS-series CS1D Duplex System Operation Manual（Cat. No. W405）.

Moreover, OMRON recommends that customers take the following measures.

- 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, limiting access to FINS port (9600)) 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.

2. 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.

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.

■ Contact information

Please contact our sales office or distributors.
https://www.ia.omron.com/global_network/index.html

■ Update history

- April 17, 2023: New Release