

Vulnerabilities related to bypass of user memory protection function of CS/CJ/CP-series Programmable Controllers

Release date: March 13, 2023
OMRON Corporation

■ Overview

Improper Access Control (CWE-284) vulnerabilities exist in the CS/CJ/CP-series Programmable Controllers.

An attacker may use these vulnerabilities to bypass protection system of the user memory (UM), disable a password, overwrite a new password, and overwrite a code for executing the user program (object code) or a function block.

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

Product series	Model	Version
SYSMAC CP-series	CP2E-E[][]D[]-[] CP2E-S[][]D[]-[] CP2E-N[][]D[]-[]	All versions
	CP1H-X40D[]-[] CP1H-XA40D[]-[] CP1H-Y20DT-D	All versions
	CP1L-EL20D[]-[] CP1L-EM[][]D[]-[] CP1L-L[][]D[]-[] CP1L-M[][]D[]-[]	All versions
	CP1E-E[][]D[]-[] CP1E-NA[][]D[]-[]	All versions

■ Description

Improper Access Control (CWE-284) vulnerabilities exist in the CS/CJ/CP-series Programmable Controllers.

■ Potential threats and impacts

An attacker may use these vulnerabilities to bypass protection system of the user memory (UM), disable a password, overwrite a new password, and overwrite a code for executing the user program (object code) or a function block.

■ CVSS Scores

Improper Access Control (CWE-284)

CVE-2023-0811

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H Base Score 9.1

■ Countermeasures

If the following products are used, you can take measures to these vulnerabilities by implementing the following measure 1) and 2).

- 1) Enable the hardware switch to prohibit writing UM. (DIP switch on front panel of the CPU Unit)

Product series	Model	Version	Manual
Programmable Controller SYSMAC CJ-series	CJ2H-CPU6[]-EIP CJ2H-CPU6[]	All versions	Refer to 3-1 CPU Units in the CJ-series CJ2 CPU Unit Hardware User's Manual (Cat. No. W472) .
	CJ2M-CPU[][]	All versions	
	CJ1G-CPU[][]P	All versions	Refer to 6-1 Overview in the CJ-series Programmable Controllers Operation Manual (Cat. No. W393).
SYSMAC CS-series	CS1H-CPU[][]H CS1G-CPU[][]H	All versions	Refer to 6-1 DIP Switch Settings in the CS-series Programmable Controllers Operation Manual (Cat. No. W339) .
	CS1D-CPU[][]HA CS1D-CPU[][]H	All versions	Refer to 2-4 CPU Units in the CS-series CS1D Duplex System Operation Manual (Cat. No. W405) .
	CS1D-CPU[][]SA CS1D-CPU[][]S	All versions	
	CS1D-CPU[][]P	All versions	
SYSMAC CP-series	CP1H-X40D[]-[] CP1H-XA40D[]-[] CP1H-Y20DT-D	All versions	Refer to 6-6-2 Write Protection in the CP-series CP1H CPU Unit Operation Manual (Cat. No. W450) .

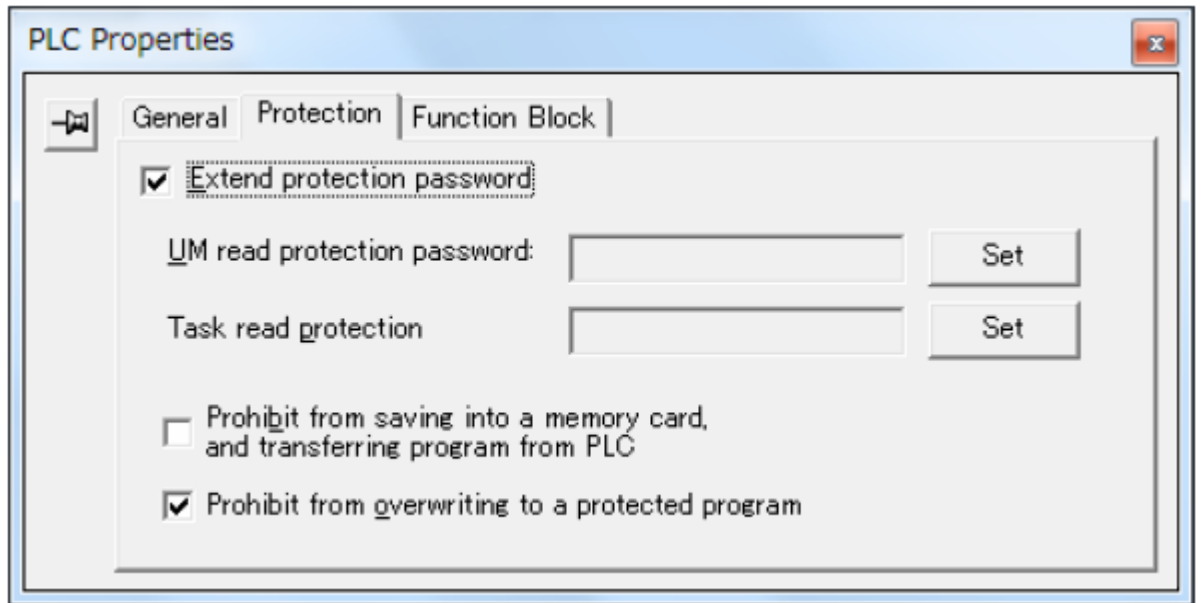
Product series	Model	Version	Manual
SYSMAC CP-series	CP1L-EL20D[]-[] CP1L-EM[][]D[]-[]	All versions	Refer to 8-7-2 Write Protection in the CP-series CP1L-EL/EM CPU Unit Operation Manual (Cat. No. W516) .
	CP1L-L[][]D[]-[] CP1L-M[][]D[]-[]	All versions	Refer to 6-7-2 Write Protection in the CP-series CP1L CPU Unit Operation Manual (Cat. No. W462) .

2) Set UM read protection password and “Prohibit from overwriting to a protected program” option.

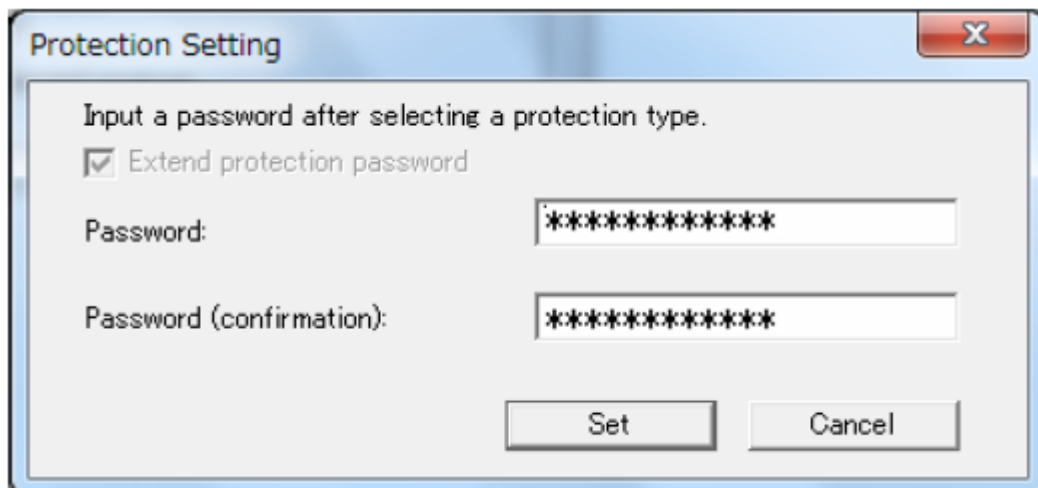
Product series	Model	Version
Programmable Controller SYSMAC CJ-series	CJ2H-CPU6[]-EIP CJ2H-CPU6[]	All versions
	CJ2M-CPU[][]	All versions
	CJ1G-CPU[][]P	Unit version 2.0 or lower
SYSMAC CS-series	CS1H-CPU[][]H CS1G-CPU[][]H	Unit version 2.0 or lower
	CS1D-CPU[][]SA CS1D-CPU[][]S	All versions
	SYSMAC CP-series	CP1H-X40D[]-[] CP1H-XA40D[]-[] CP1H-Y20DT-D
CP1L-EL20D[]-[] CP1L-EM[][]D[]-[] CP1L-L[][]D[]-[] CP1L-M[][]D[]-[]		All versions

For the relevant function, refer to Applying a Password to the PLC Programs in the CX-Programmer Ver.9.[.] Operation Manual (Cat. No. W446) .

1. Register a password from PLC Properties.
 - 1) Select the Extend protection password Check Box on the Protection Tab in the PLC Properties Dialog Box with the CX-Programmer. (For the strong protection, OMRON recommends using the extended read protection function.)
 - 2) Select the Prohibit from overwriting to a protected program Check Box.
 - 3) Select the Set Button on the right side of the UM read protection password.



- 4) Input a password in the Protection Setting Dialog Box, and then select the Set Button.



- 5) Close the PLC Properties Dialog Box.
2. Connect online and make read protection to PLC.

■ Mitigations and Protections

If the above countermeasures cannot be applied, OMRON recommends that customers take the following mitigation measures.

1. Security measures to prevent unauthorized access

- If the following products and versions are used, the risk of attacks by an attacker via the network can be reduced by taking the following measure 1) and 2).

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).

Product series	Model	Version	Manual
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) .
SYSMAC CP-series	CP1H-X40D[]-[] CP1H-XA40D[]-[] CP1H-Y20DT-D	All versions	Refer to 6-6-2 Write Protection in the CP-series CP1H CPU Unit Operation Manual (Cat. No. W450) .

2) Select the Protect by IP Address.

Product series	Model	Version	Manual
Programmable Controller SYSMAC CP-series	CP2E-N[][]D[]-[]	All versions	Refer to 15-4-4 PLC Setup for FINS/UDP and FINS/TCP Applications in the CP-series CP2E CPU Unit Software User's Manual (Cat. No. W614) .

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

■ Acknowledgement

These vulnerabilities were reported by Mr. Sam Hanson who belongs to Dragos through CISA (Cybersecurity & Infrastructure Security Agency). OMRON is grateful to Mr. Sam Hanson for finding and reporting these vulnerabilities.

■ Update history

- March 13, 2023: New Release