Multiple vulnerabilities caused by OpenSSL in CS/CJ-series Programmable Controllers EtherNet/IP Unit

Release date: November 1, 2024
OMRON Corporation

■Overview

Use of Observable Discrepancy (CWE-203), Double Free (CWE-415), and Use After Free (CWE-416) vulnerabilities exist in CS/CJ-series Programmable Controllers EtherNet/IP Unit. If an attacker uses these vulnerabilities, the information about the controller product may be leaked or the controller product may go into a denial of service (DoS) state.

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.

Model	Version	Lot No. (Date of Manufacture)
CS1W-EIP21S	Ver.1.02 or lower	Until 241014 (October 14, 2024)
CJ1W-EIP21S	Ver.1.02 or lower	Until 241014 (October 14, 2024)

Refer to the “Lot Numbers and Unit Versions of CS/CJ-series” in the “EtherNet/IP Units Operation Manual (W465)” to check the product version and the lot number.

■Description

Due to the multiple vulnerabilities caused by OpenSSL in CS/CJ-series Programmable Controllers EtherNet/IP Unit, the information about the controller product may be leaked or the controller product may go into a denial of service (DoS) state.

■CVSS Scores

1) Observable Discrepancy (CWE-203)
CVE-2022-4304
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N Base Score 5.9

2) Double Free (CWE-415)
CVE-2022-4450
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score 7.5

3) Use After Free (CWE-416)
CVE-2023-0215
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score 7.5

■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.

Model	Version	Lot No.	Release Date
CS1W-EIP21S	Ver.1.03 or higher	241015 or later	October 15, 2024
CJ1W-EIP21S	Ver.1.03 or higher	241015 or later	October 15, 2024

For information on how to obtain and update the firmware for the countermeasure version of the product, please contact our sales office or distributors.

■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.

■Contact information

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

■Update history

- November 1, 2024: New Release