Vulnerability that could cause a Denial of Service (DoS) state in the built-in EtherNet/IP™ port of the CJ Series CJ2 CPU unit and the CS/CJ series EtherNet/IP™ unit

Release date: August 1, 2023
Last modified on November 13, 2023
OMRON Corporation

■Overview

Improper Validation of Specified Type of Input (CWE-1287) vulnerability exist in the built-in EtherNet/IP™ port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP™ unit that could cause the unit to be put into a Denial of Service (DoS) state by sending a malformed packet.

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
CJ2M CPU Unit	CJ2M-CPU3[]	Unit version of the built-in EtherNet/IP™ section Ver. 2.18 or lower
CJ2H CPU Unit	CJ2H-CPU6[]-EIP	Unit version of the built-in EtherNet/IP™ section Ver. 3.04 or lower
CS/CJ Series EtherNet/IP™ Unit	CS1W-EIP21 CJ1W-EIP21	Ver. 3.04 or lower

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

CJ Series CPU Unit User's Manual (Hardware)（W472-E1-15）

Refer to “Unit Versions of CJ2 CPU Units” section in the above manuals.

CS/CJ Series EtherNet/IP™ Units Operation Manual（W465-E1-12）

Refer to “Unit Versions of CS/CJ-series” section in the above manuals.

■Description

Improper Validation of Specified Type of Input (CWE-1287) vulnerability exist in the built-in EtherNet/IP™ port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP™ unit that could cause the unit to be put into a Denial of Service (DoS) state by sending a malformed packet.

■Potential threats and impacts

An attacker may use the vulnerability to bring the unit Denial of Service (DoS) state.

■CVSS Score

CWE-1287: Improper Validation of Specified Type of Input

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H 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
CJ2M CPU Unit	CJ2M-CPU3[]	Unit version of the built-in EtherNet/IP™ section Ver. 2.19 or upper	June 16, 2023
CJ2H CPU Unit	CJ2H-CPU6[]-EIP	Unit version of the built-in EtherNet/IP™ section Ver. 3.05 or upper	August 1, 2023
CS/CJ Series EtherNet/IP™ Unit	CS1W-EIP21 CJ1W-EIP21	Ver. 3.05 or upper	August 1, 2023

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

■Update History

- August 1, 2023: New Release
- September 1, 2023: Corrected countermeasure version release date for CJ2H CPU Unit and CS/CJ Series EtherNet/IP™ Unit
- November 13, 2023: Corrected method of obtaining countermeasures