

Vulnerabilities in Omron CJ series PLCs

Omron Corporation

February 28, 2020

Thank you for your use of Omron's programmable controllers (PLC).

An external institution pointed out vulnerabilities in our PLCs: one in the FINS protocol function. We would kindly ask you to read the details below and take countermeasures to avoid risks.

1. Affected Equipment

- All versions of CJ series PLCs

2. Details of Vulnerabilities

2.1 Vulnerability in the FINS protocol against DoS attack

- CVE-2020-6986: FINS protocol has a risk of flooding attack by malformed packet

CWE: CWE-400 Uncontrolled Resource Consumption

CVSSv3 : 7.5(High) CVSS:7.5/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CJ series PLCs have vulnerability related to improper resource management in excessive malformed packet processing.

3. Countermeasures

To avoid the risk of attacks from windows of those vulnerabilities, we have asked our customers to adopt the following countermeasures by themselves:

- 1) Antivirus protection
- 2) Data input/output protection
- 3) Data backup
- 4) Protection against computer virus for Omron products and installed software
- 5) Adequate prevention against illegal access to Omron products

For instance, a firewall to protect devices from an external network, network access restriction by VPN, filtering a well-known communication port (FINS communication port is 9600, default) in the network side, or other proper security measures are recommended.

Omron will keep improving product security. We appreciate your continuous loyalty for our products.