

## Vulnerabilities in Omron CS and CJ series CPU PLCs

Omron Corporation

December 6, 2019

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

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

### 1. Affected Equipment

- All versions of CS series CPU and CJ series CPU
- NJ series CPU (FTP function)

### 2. Details of Vulnerabilities

#### 2.1 Multiple vulnerabilities in the FINS communication protocol

FINS communication packet between a controller and a PLC may be monitored and it may invite replay attack using commands for the PLC. Vulnerabilities are described in the following.

- ICS-VU-612969: Password on UM of FINS

CWE: CWE-290 Authentication Bypass by Spoofing

CVSSv3: 5.6 (Medium) CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L

Omron's CS and CJ series PLCs have vulnerability that an ID-theft may be authenticated.

- ICS-VU-683468: FINS protocol

CWE: CWE-294 Authentication Bypass by Capture-replay

CVSSv3: 8.6 (High) CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

Omron's CS and CJ series PLCs have vulnerability that some functions may be executed unintentionally.

- ICS-VU-033046: Incomplete check on FINS header (CJ2M)

CWE: CWE-940: Improper Verification of Source of a Communication Channel

CVSSv3: 8.6 (High) CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

Omron's CS and CJ series PLCs have vulnerability that communication channel sources are verified inadequately.

## 2.2 Vulnerability in the FTP function

- ICS-VU-326877: FTP password authentication has a risk of brute-force attack  
CWE: CWE-307 Improper Restriction of Excessive Authentication Attempts  
CVSSv3: 6.5 (Medium) CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N  
Omron's CS and CJ series PLCs have vulnerability regarding restriction for over trials of authentication.

## 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.