Vulnerabilities in Omron PLCs

Omron Corporation
Release date: December 6, 2019
Last modified on January 10, 2023

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 Units
   - All versions of CJ series CPU Units
   - All versions of NJ series CPU Units (except CVE-2019-18269)
   - All versions of NX series CPU Units (except CVE-2019-18269)

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.

・Authentication Bypass by Spoofing

CWE: CWE-290 Authentication Bypass by Spoofing

CVE: CVE-2019-18259

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, CJ, NJ and NX series PLCs have vulnerability that an ID-theft may be authenticated.

・Authentication Bypass by Capture-replay

CWE: CWE-294 Authentication Bypass by Capture-replay

CVE: CVE-2019-13533

CVSSv3: 8.1（High）CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L
Omron's CS, CJ, NJ and NX series PLCs have vulnerability that some functions may be executed unintentionally.

・Vulnerability in password on UM of FINS
CWE-412 Unrestricted Externally Accessible Lock
CVE：CVE-2019-18269
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 unrestricted externally accessible lock vulnerability.

2.2 Vulnerability in the FTP function

・FTP password authentication has a risk of brute-force attack
CWE: CWE-307 Improper Restriction of Excessive Authentication Attempts
CVE: CVE-2019-18261
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, CJ, NJ and NX 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, FTP communication port is 21, default) in the network side, using Omron's PLC function such as packet filtering / disabling unused protocol or other proper security measures are recommended.

4. Acknowledgments

Japing You (XDU) and n0b0dy reported us via CISA the multiple vulnerabilities in the FINS communication protocol vulnerabilities.

n0b0dy reported us via CISA the vulnerability in the FTP function.

Pawan Sable and Dr. Faruk Kazi from COE-CNDS Lab, VJTI Mumbai, India in the Security Advisory (SA) reported us via CERT-In and JPCERT/CC the vulnerability in the FINS protocol in NX1P2.

Many thanks to all reporters.

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

Date	History
December 6, 2019	New Release
November 24, 2022	Change of Title 1. Update of affected devices 2.1 FINS protocol: Correction of erroneous CVSS value and addition of model
December 2, 2022	2. Details of Vulnerabilities: Added CVE IDs 2.3 Incomplete check on FINS header (CJ2M): Correction of erroneous CWE. Added 4. Acknowledgments
December 8, 2022	Modified 4. Acknowledgments
January 10, 2023	1. Update of affected devices 2.1 Multiple vulnerabilities in the FINS communication protocol: Correction of erroneous descriptions and addition of model 2.2 Vulnerability in the FTP function: update of affected devices 3. Update of Countermeasures