Authentication bypass vulnerabilities in communications functions of NJ/NX-series Machine Automation Controllers

Release date: July 1, 2022
Last modified on October 11, 2022
OMRON Corporation

■Overview

Use of Hard-coded Credentials (CWE-798) and Authentication Bypass by Capture-replay (CWE-294) vulnerabilities exist in the communications functions between the NJ/NX-series Machine Automation Controllers, Automation software Sysmac Studio, and NA-series Programmable Terminals. An attacker may use these vulnerabilities to bypass authentication in the communications connection process and perform unauthorized access to the controller products.

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
NX7-series Machine Automation Controller	All models	1.28 or lower
NX1-series Machine Automation Controller	All models	1.48 or lower
NJ-series Machine Automation Controller	All models	1.48 or lower
Automation Software Sysmac Studio	All models	1.49 or lower
NA-series Programable Terminal	NA5-15W NA5-12W NA5-9W NA5-7W	Runtime version 1.15 or lower

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

・ NX-series CPU Unit Hardware User's Manual (W535)
・ NX-series NX102 CPU Unit Hardware User's Manual (W593)
・ NX-series NX1P2 CPU Unit Hardware User's Manual (W578)
・ NJ-series CPU Unit Hardware User's Manual (W500)
Refer to "Checking Versions" section in the above manuals.

・ NA-series Programmable Terminal Hardware User's Manual (V117)
・ NA-series Programmable Terminal Hardware(-V1) User's Manual (V125)
Refer to "System Menu Overview" section in the above manuals. (The Runtime version is found on the left bottom area of the System Menu screen.)

・ Sysmac Studio Version 1 Operation Manual (W504)
Refer to "Displaying and Registering Licenses" section in the above manual.

■Description

Due to the Use of Hard-coded Credentials (CWE-798) and Authentication Bypass by Capture-replay (CWE-294) vulnerabilities which exist in the communications functions between the NJ/NX-series Machine Automation Controllers, Automation software Sysmac Studio, and NA-series Programmable Terminals, the products may be logged in and operated without authorization.

■ Potential threats and impacts

An attacker may use the vulnerabilities to bypass authentication in the communications connection process and login and operate the controller products without authorization.

■ CVSS Scores

1) Use of Hard-coded Credentials (CWE-798)
CVE-2022-34151
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H Base Score 9.4

2) Authentication Bypass by Capture-replay (CWE-294)
CVE-2022-33208
CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/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
NX7-series Machine Automation Controller	All models	1.29 or higher	October 11, 2022
NX1-series Machine Automation Controller	All models	1.50 or higher	October 11, 2022
NJ-series Machine Automation Controller	NJ501-1300 NJ501-1400 NJ501-1500	1.49 or higher	July 1st, 2022
	Other than above models	1.50 or higher	October 11, 2022
Automation Software Sysmac Studio	All models	1.50 or higher	July 1st, 2022
NA-series Programable Terminal	NA5-15W NA5-12W NA5-9W NA5-7W	Runtime version 1.16 or higher	July 1st, 2022

For information on how to obtain and update the firmware for the countermeasure version of the product, please contact our sales office or distributors. You can update the Sysmac Studio to the latest versions using the installed Omron Automation Software AutoUpdate tool.

It is recommended to take countermeasures using the following security functions of the Controller. For details on the function and how to set it, refer to *8-5 Security* in the *NJ/NX-series CPU Unit Software User’s Manual (Cat. No. W501)*.

- Use the secure communication function to encrypt communication data between the Sysmac Studio or NA-series Programmable Terminal and the Controller. By doing so, it is possible to prevent data interception or alteration by a third party.
- Use the Packet Filter function to filter IP packets in the reception process of the built-in EtherNet/IP port. By doing so, it is possible to restrict unauthorized access from the outside.
- Use the user authentication function to authenticate individual users when the tool is connected online and prevent unauthorized access by allowing only operations according to authority.

■Contact information

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

■Others

These vulnerabilities and countermeasures in this document correspond to the vulnerabilities used by the vulnerability attack tools and countermeasures that are reported below by the US Cybersecurity & Infrastructure Security Agency (CISA).

APT Cyber Tools Targeting ICS/SCADA Devices
https://www.cisa.gov/uscert/ncas/alerts/aa22-103a

■Update history

- July 1, 2022: New Release
- October 11, 2022: Made changes on the following.

(1) The release date in *Countermeasures* was changed.

(2) With the review of vulnerability assessment, changed the following.

- CVSS score of CVE-2022-34151

  (Before change) CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:H Base Score 7.7
  (After change) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H Base Score 9.4

- CWE ID and CVSS Score of CVE-2022-33208

  (Before change) CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:H/A:H Base Score 6.2
  (After change) CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H Base Score 7.5