

Malicious program execution vulnerability in NJ/NX-series Machine Automation Controllers

Release date: July 1, 2022

Last modified on October 11, 2022

OMRON Corporation

■ Overview

Active Debug Code (CWE-489) vulnerability exists in the NJ/NX-series Machine Automation Controllers. An attacker may illegally access the controllers and use the vulnerability to cause the product to be out of service state or execute a malicious program.

The products and versions affected by the vulnerability, mitigation and protection measures are shown below. Make sure to implement these recommended mitigations and protections to minimize the risk of exploitation of this vulnerability. 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

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.

■ Description

Due to the Active Debug Code (CWE-489) vulnerability which exists in the NJ/NX-series Machine Automation Controllers, the controllers may be put in out of service state or a malicious program may be executed.

■ Potential threats and impacts

An attacker may use the vulnerability to cause the product to be out of service state or execute a malicious program.

■ CVSS Score

CVE-2022-33971

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H Base Score 8.3

■ Mitigations and Protections

OMRON recommends that customers take the following mitigation measures to minimize the risk of exploitation of this vulnerability.

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 vulnerability can be implemented by updating each product firmware to the countermeasure version. The firmware updates are highly recommended. The countermeasure version and respective release date for each product are 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 1 st , 2022
	Other than above models	1.50 or higher	October 11, 2022

For information on how to obtain and update the product firmware, 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.

■ Contact information

Please contact our sales office or distributors.

https://www.ia.omron.com/global_network/index.html

■ Others

This vulnerability 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 CWE ID and CVSS Score of CVE-2022-33971.

(Before change) Authentication Bypass by Capture-replay (CWE-294)

CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H Base Score 7.6

(After change) Active Debug Code (CWE-489)

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H Base Score 8.3