Least Privilege Violation Vulnerability in the communications functions of NJ/NX-series Machine Automation Controllers

Release date: July 14, 2025
OMRON Corporation

■Overview

Least Privilege Violation (CWE-272) Vulnerability exists in the communication function between the NJ/NX-series Machine Automation Controllers and the Sysmac Studio Software. An attacker may use this vulnerability to perform unauthorized access and to execute unauthorized code remotely to the controller products.

The products and versions affected by this 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 countermeasure shown below in this document and implement appropriate countermeasure.

■Affected products

Affected products and versions are below.

Machine Automation Controller NJ-series

Model	Version	Lot No. (Date of Manufacture)
NJ101-[][][][]	Ver.1.67.00 or lower	Until 13725 (July 13, 2025)
NJ301-1[]00	Ver.1.67.00 or lower	
NJ501-1[]00	Ver.1.67.02 or lower	
NJ501-1[]20	Ver.1.68.01 or lower	
NJ501-1340	Ver.1.67.00 or lower	
NJ501-4[][][]	Ver.1.67.00 or lower	
NJ501-5300	Ver.1.67.01 or lower	
NJ501-R[]00	Ver.1.67.01 or lower	
NJ501-R[]20	Ver.1.67.00 or lower	

Refer to the appendix for how to check the target product version.

Refer to the “ID Information Indication” section in the above manuals for how to check the lot number.

- NJ-series CPU unit Hardware User’s Manual (W500)

Machine Automation Controller NX-series

Model	Version	Lot No. (Date of Manufacture)
NX102-[][][][]	Ver.1.68.01 or lower	Until 13725 (July 13, 2025)
NX1P2-[][][][][][]	Ver.1.64.09 or lower	
NX1P2-[][][][][][]1	Ver.1.64.09 or lower	
NX502-[][][][]	Ver.1.68.01 or lower	
NX701-[][][][]	Ver.1.35.09 or lower	

Refer to the appendix for how to check the target product version.

Refer to the “ID Information Indication” section in the above manuals for how to check the lot number.

- NX102 CPU Unit User’s Manual (Hardware) (W593)
- NX1P2 CPU Unit User’s Manual (Hardware) (W578)
- NX5 CPU Unit User’s Manual (Hardware) (W629)
- NX7 CPU Unit User’s Manual (Hardware) (W535)

Sysmac Studio Software

Model	Version
SYSMAC-SE2[][][]	All

Refer to “Displaying and Registering Licenses” section in the above manual to check the product version.

- Sysmac Studio Version 1 Operation Manual (W504)

■Description

Due to Least Privilege Violation (CWE-272) Vulnerability which exists in NJ/NX-series Machine Automation Controllers, the products may be performed unauthorized access and RCE (Remote Code Execution).

■CWE,CVE,CVSS Scores

Least Privilege Violation(CWE-272)

CVE-2025-1384

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:H Base Score 7.0

■Countermeasure

The countermeasure against the vulnerability can be implemented by updating each product to the countermeasure version and setting the secure communication version 2.

1. Update the product to the security enhanced countermeasure version

The countermeasure version and respective release date for each product is shown in the table below.

Machine Automation Controller NJ-series

Model	Version	Lot No.	Release Date
NJ101-[][][][]	Ver.1.69.00 or higher	14725 or later	July 14, 2025
NJ301-1[]00			
NJ501-1[]00			
NJ501-1[]20			
NJ501-1340			
NJ501-4[][][]			
NJ501-5300			
NJ501-R[]00			
NJ501-R[]20			

For information on how to obtain and update the firmware for the countermeasure version of the product, please contact our sales office or distributors.

Machine Automation Controller NX-series

Model	Version	Lot No.	Release Date
NX102-[][][][]	Ver.1.69.00 or higher	14725 or later	July 14, 2025
NX1P2-[][][][][][]			
NX1P2-[][][][][][]1			
NX502-[][][][]			
NX701-[][][][]	Ver.1.36.00 or higher		

For information on how to obtain and update the firmware for the countermeasure version of the product, please contact our sales office or distributors.

Sysmac Studio Software

Model	Version	Release Date
SYSMAC-SE2[][][]	Ver.1.69.00 or higher	July 14, 2025

You can update to the latest versions using the installed Omron Automation Software AutoUpdate tool.

2. Set the secure communication version 2

The secure communication version can be set online for the first time in Sysmac Studio or from the secure communication settings screen. For details on how to set the secure communication version, refer to Sysmac Studio Version 1 Operation Manual (W504).

■ Mitigations and Protections

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

1. Secure Communication Function

   The secure communication function can prevent data from being eavesdropped or tampered with by a third party. Secure communication is available in the following CPU Units of the stated versions.
   - NJ series, NX102, NX1P2 CPU Unit: Version 1.49 or higher
   - NX701 CPU Unit: Version 1.29 or higher
   - NX502 CPU Unit: Version 1.60 or higher

2. 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.

3. 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.

4. 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.

5. Data recovery
   Periodical data backup and maintenance to prepare for data loss.

■Contact information

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

■Acknowledgment

Tamir Ariel, CPS Research Team, Microsoft reported this vulnerability.
Thanks to Tamir Ariel for finding and reporting it.

■Update history

- July 14, 2025: New Release

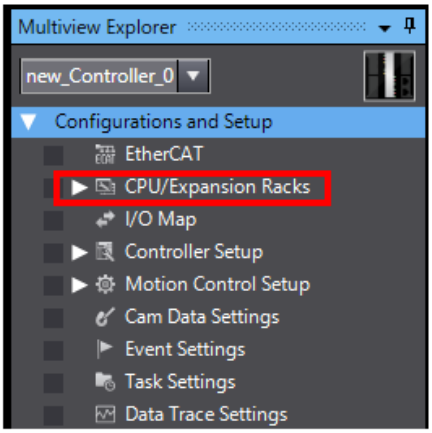
Appendix How to check the product version

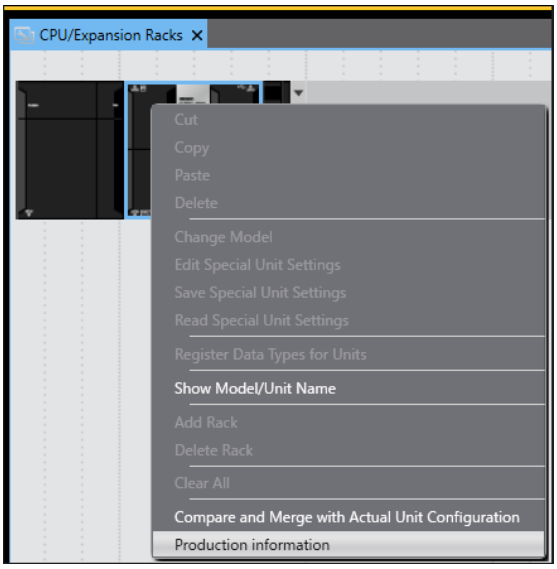
The method of checking the product version varies depending on the series.

For NJ-series

Double-click **CPU/Expansion Racks** under **Configurations and Setup** in the Multiview Explorer.

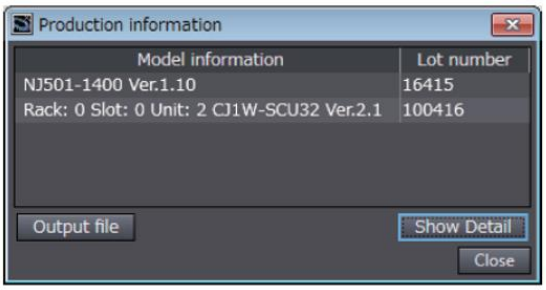
Right-click any open space in the Unit Editor and select **Production Information**.

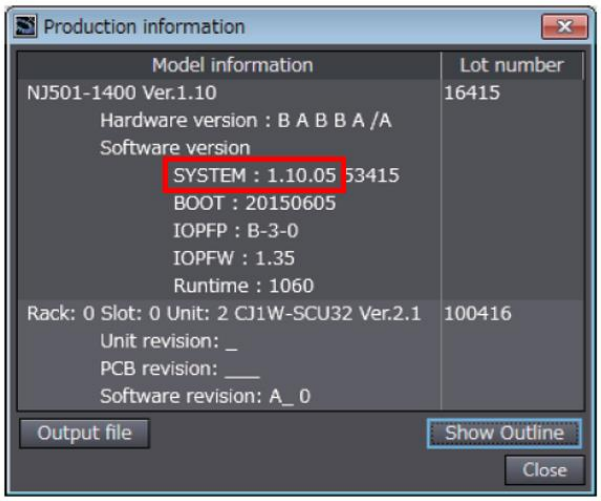




Click the **Show Detail** Button at the lower right of the Production Information Dialog Box.

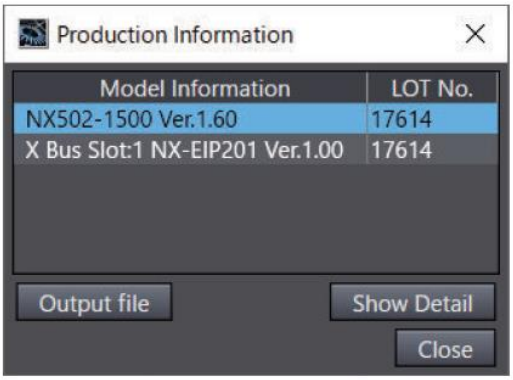
The figure below shows Ver.1.10.05.





For NX-series

Right-click **CPU Rack** under **Configurations and Setup** - **CPU/Expansion Racks** in the Multiview Explorer and select **Display Production Information**. The **Production Information** Dialog Box is displayed.



Click the **Show Detail** or **Show Outline** Button at the lower right of the **Production Information** Dialog Box. The view will change between the production information details and outline. The figure below shows Ver.1.60.02(NX502-1500) and Ver.1.00.00(NX-EIP201).