

Path Traversal Vulnerabilities in NJ/NX-series Machine Automation Controllers

Release date: January 14, 2025

OMRON Corporation

■ Overview

Path Traversal Vulnerabilities (CWE-22) exist in NJ/NX-series Machine Automation Controllers. An attacker may use these vulnerabilities to perform unauthorized access and to execute unauthorized code remotely 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 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.1.64.05 or lower	Until 30924 (September 30, 2024)
NJ301-[] [] [] []		
NJ501-1 [] 0 []		
NJ501-1 [] 2 []	ver.1.64.04 or lower	
NJ501-1340		
NJ501-4 [] [] []		
NJ501-5300		
NJ501-R [] [] []		

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)
NX1P2-[] [] [] [] [] []	Ver.1.64.04 or lower	Until 19Y24 (November 19, 2024)
NX1P2-[] [] [] [] [] [] 1	Ver.1.64.04 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.

- NX1P2 CPU Unit User’s Manual (Hardware) (W578)

■ Description

Due to the Path Traversal Vulnerabilities (CWE-22) which exist in NJ/NX-series Machine Automation Controllers, the products may be performed unauthorized access and RCE (Remote Code Execution).

■ CVSS Scores

Path Traversal (CWE-22)

CVE-2024-12083

CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H Base Score 6.6

■ Countermeasure

The countermeasure 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.

Machine Automation Controller NJ-series

Model	Version	Lot No.	Release Date
NJ101-[] [] [] []	Ver.1.67.00 or higher	01X24 or later	October 1, 2024
NJ301-[] [] [] []			
NJ501-1[] 0 []			
NJ501-1[] 2 []			
NJ501-1340			
NJ501-4[] [] []			
NJ501-5300			
NJ501-R[] [] []			

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
NX1P2-[[[[]]][]]	Ver.1.64.06 or higher	20Y24 or later	November 20, 2024
NX1P2-[[[[]]][]]1			

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

■ Mitigations and Protections

OMRON recommends that customers take the following mitigation measures to minimize the risk of exploitation of these vulnerabilities.

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, NX1P2 CPU Unit: Version 1.49 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

■ Update history

- January 14, 2025: New Release

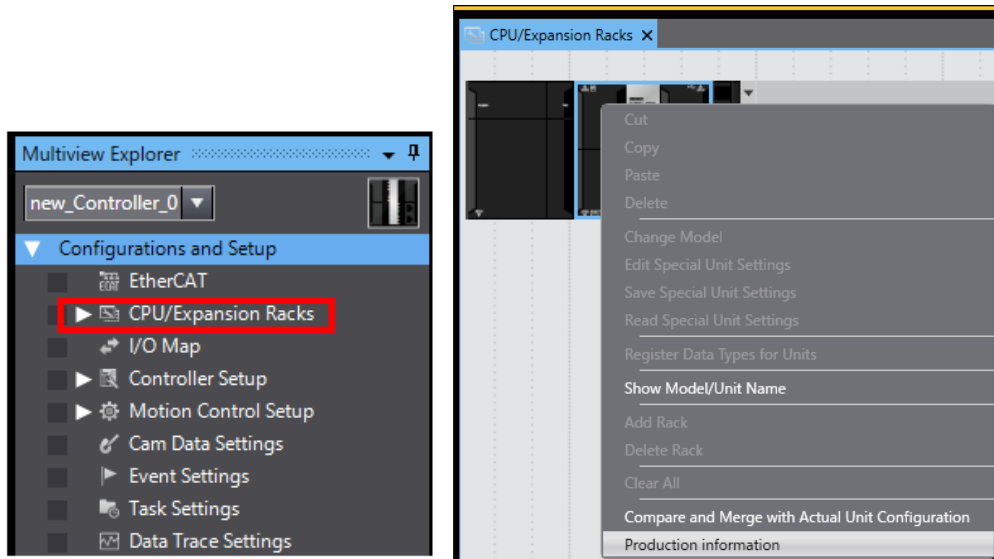
Appendix How to check the product version

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

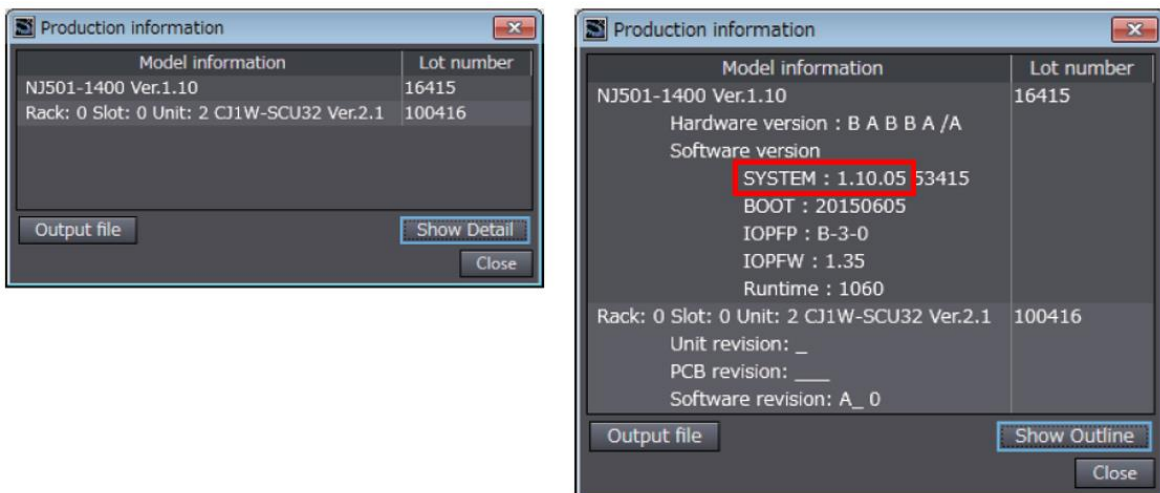
For NJ-series

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**.

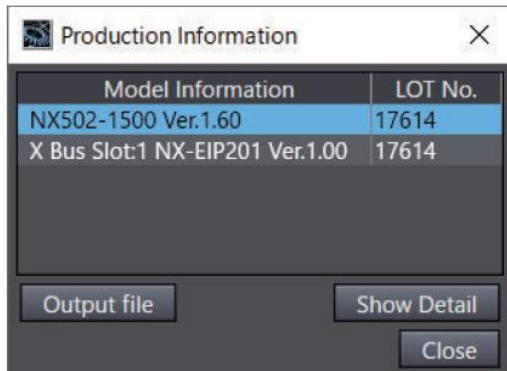


Click the **Show Detail** Button at the lower right of the Production Information Dialog Box. The figure below shows Ver.1.10.05.



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).

