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

Release date: March 7, 2024
Last modified on May 27, 2024
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.1.64.03 or lower	Until 25424 (April 25, 2024)
NJ301-[][][][]	Ver.1.64.00 or lower	
NJ501-1[]0[]	Ver.1.64.03 or lower	
NJ501-1[]2[]	Ver.1.64.00 or lower	
NJ501-1340	Ver.1.64.00 or lower	
NJ501-4[][][]	Ver.1.64.00 or lower	
NJ501-5300	Ver.1.64.00 or lower	
NJ501-R[][][]	Ver.1.64.00 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.1.64.00 or lower	Until 25424 (April 25, 2024)
NX1P2-[][][][][][]	Ver.1.64.00 or lower	
NX1P2-[][][][][][]1	Ver.1.64.00 or lower	
NX502-[][][][]	Ver.1.65.01 or lower	
NX701-[][][][]	Ver.1.35.00 or lower	
NX-EIP201	Ver.1.00.01 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)
- NX-EIP201 EtherNet/IP^{TM} Units User’s Manual (W627)

■ 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-2024-27121

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H Base Score 7.2

■ 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.1.64.04 or higher	26424 (April 26, 2024) or later
NJ301-[][][][]	Ver.1.64.04 or higher	
NJ501-1[]0[]	Ver.1.64.04 or higher	
NJ501-1[]2[]	Ver.1.64.04 or higher	

NJ501-1340	Ver.1.64.04 or higher	
NJ501-4[][][]	Ver.1.64.04 or higher	
NJ501-5300	Ver.1.64.04 or higher	
NJ501-R[][][]	Ver.1.64.04 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.

Machine Automation Controller NX-series

Model	Version	Lot No. (Date of Manufacture)
NX102-[][][][]	Ver.1.64.04 or higher	26424 (April 26, 2024) or later
NX1P2-[][][][][][]	Ver.1.64.04 or higher	
NX1P2-[][][][][][]1	Ver.1.64.04 or higher	
NX502-[][][][]	Ver.1.66.01 or higher	
NX701-[][][][]	Ver.1.35.04 or higher	
NX-EIP201	Ver.1.01.00 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.

■ 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, 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
   - NX-EIP201 : Ver.1.00 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, and Logan Carpenter, Principle Vulnerability Analyst, Dragos, reported these vulnerabilities.
Thanks to Tamir Ariel and Logan Carpenter for finding and reporting them.

■Update history

- March 7, 2024: New Release
- May 27, 2024: Update the Lot No. of affected products and countermeasure version.

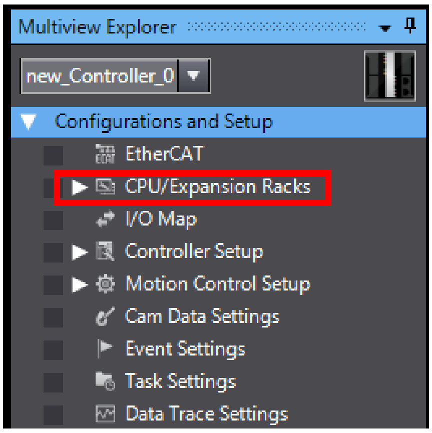
Appendix How to check the product version

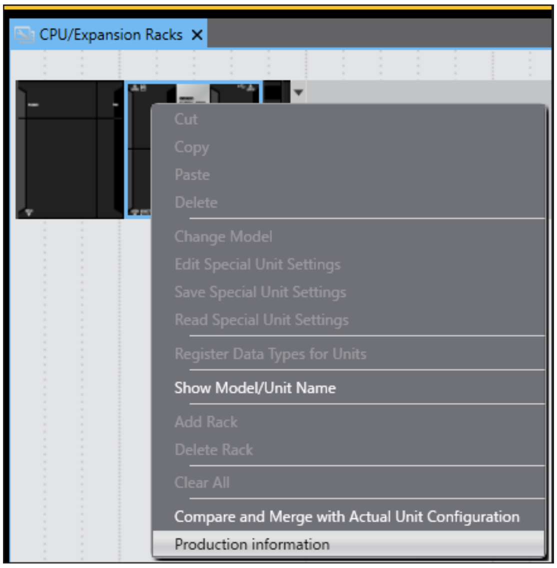
The method of checking the product version varies depending on the series.

For NJ-series

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

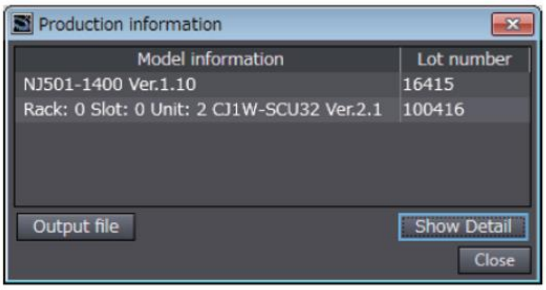
Right-click any open space in the Unit Editor and select **Production Information**.



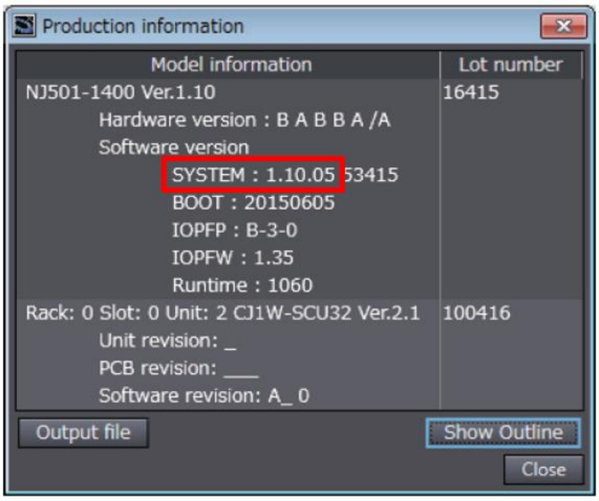

CPU/Expansion Racks
Cut
Copy
Paste
Delete
Change Model
Edit Special Unit Settings
Save Special Unit Settings
Read Special Unit Settings
Register Data Types for Units
Show Model/Unit Name
Add Rack
Delete Rack
Clear All
Compare and Merge with Actual Unit Configuration
Production information

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

The figure below shows Ver.1.10.05.



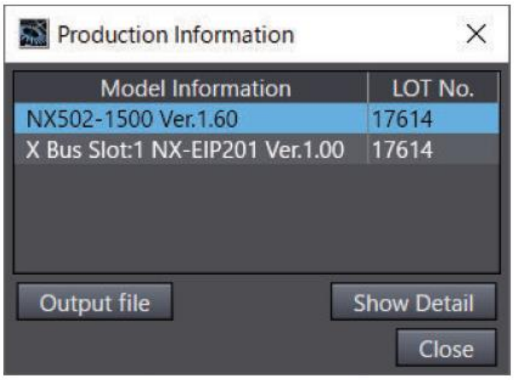
Model information	Lot number
NJ501-1400 Ver.1.10	16415
Rack: 0 Slot: 0 Unit: 2 CJ1W-SCU32 Ver.2.1	100416



Model information	Lot number
NJ501-1400 Ver.1.10 Hardware version : B A B B A /A Software version SYSTEM : 1.10.05 53415 BOOT : 20150605 IOPFP : B-3-0 IOPFW : 1.35 Runtime : 1060	16415
Rack: 0 Slot: 0 Unit: 2 CJ1W-SCU32 Ver.2.1 Unit revision: _ PCB revision: ___ Software revision: A_ 0	100416

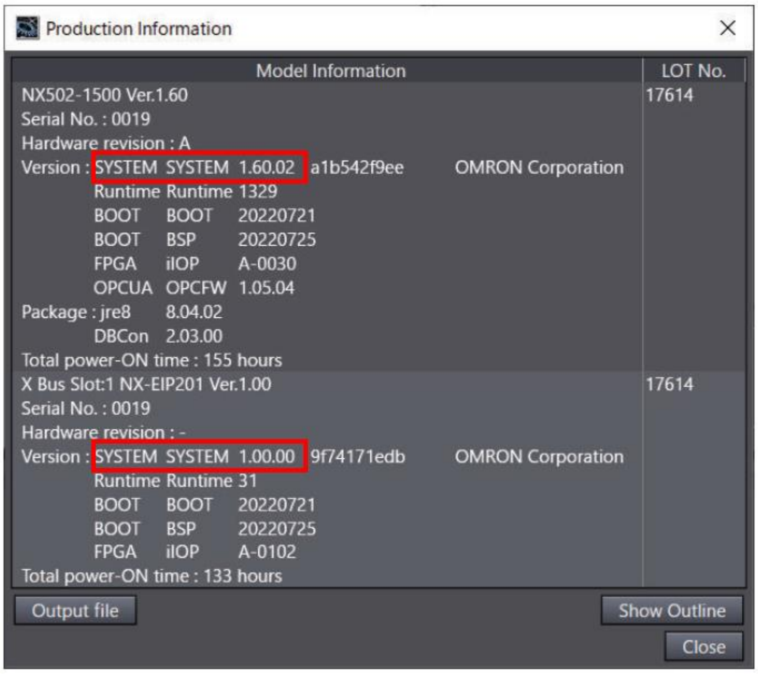
For NX-series

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.



Model Information	LOT No.
NX502-1500 Ver.1.60	17614
X Bus Slot:1 NX-EIP201 Ver.1.00	17614

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).



```
NX502-1500 Ver.1.60                                                     17614
Serial No. : 0019
Hardware revision : A
Version : SYSTEM  SYSTEM  1.60.02  a1b542f9ee        OMRON Corporation
          Runtime Runtime 1329
          BOOT    BOOT    20220721
          BOOT    BSP     20220725
          FPGA    iIOP    A-0030
          OPCUA   OPCFW   1.05.04
Package : jre8    8.04.02
          DBCon   2.03.00
Total power-ON time : 155 hours
X Bus Slot:1 NX-EIP201 Ver.1.00                                         17614
Serial No. : 0019
Hardware revision : -
Version : SYSTEM  SYSTEM  1.00.00  9f74171edb        OMRON Corporation
          Runtime Runtime 31
          BOOT    BOOT    20220721
          BOOT    BSP     20220725
          FPGA    iIOP    A-0102
Total power-ON time : 133 hours
```