Multiple vulnerabilities caused by OpenSSL

in NJ/NX-series Machine Automation Controllers

Release date: May 27, 2024

OMRON Corporation

■Overview

Use of Observable Discrepancy (CWE-203), Double Free (CWE-415), and Use After Free (CWE-416) vulnerabilities exist in NJ/NX-series Machine Automation Controllers. If an attacker uses these vulnerabilities, the information about the controller product may be leaked or the controller product may go into a denial of service (DoS) state.

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.

Machine Automation Controller NJ-series

Model	Version	Lot No. (Date of Manufacture)
NJ101-[][][][]	Ver.1.64.03 or lower	Until 25424 (Until April 25, 2024)
NJ301-[][][][]	Ver.1.64.00 or lower	Until 25424 (Until April 25, 2024)
NJ501-1[]0[]	Ver.1.64.03 or lower	Until 25424 (Until April 25, 2024)
NJ501-1[]2[]	Ver.1.64.00 or lower	Until 25424 (Until April 25, 2024)
NJ501-1340	Ver.1.64.00 or lower	Until 25424 (Until April 25, 2024)
NJ501-4[][][]	Ver.1.64.00 or lower	Until 25424 (Until April 25, 2024)
NJ501-5300	Ver.1.64.00 or lower	Until 25424 (Until April 25, 2024)
NJ501-R[][][]	Ver.1.64.00 or lower	Until 25424 (Until April 25, 2024)

Refer to the Appendix to check the product version.

Refer to the "ID Information Indication" in the following manual to check the lot number.

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

C09-27-01B

Machine Automation Controller NX-series

Model	Version	Lot No. (Date of Manufacture)
NX102-[][][][]	Ver.1.64.00 or lower	Until 25424 (Until April 25, 2024)
NX1P2-[][][][][][]	Ver.1.64.00 or lower	Until 25424 (Until April 25, 2024)
NX1P2-[][][][][][]1	Ver.1.64.00 or lower	Until 25424 (Until April 25, 2024)
NX502-[][][][]	Ver.1.65.01 or lower	Until 25424 (Until April 25, 2024)
NX701-[][][][]	Ver.1.35.00 or lower	Until 25424 (Until April 25, 2024)
NX-EIP201	Ver.1.00.01 or lower	Until 25424 (Until April 25, 2024)

Refer to the Appendix to check the product version.

Refer to the "ID Information Indication" in the following manual to check the lot number.

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

■Description

Due to the multiple vulnerabilities caused by OpenSSL in NJ/NX-series Machine Automation Controllers, the information about the controller product may be leaked or the controller product may go into a denial of service (DoS) state.

■CVSS Scores

1) Observable Discrepancy (CWE-203)

CVE-2022-4304

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N Base Score 5.9

2) Double Free (CWE-415)

CVE-2022-4450

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score 7.5

3) Use After Free (CWE-416)

CVE-2023-0215

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score 7.5

■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.

C09-27-01B

Machine Automation Controller NJ-series

Model	Version	Lot No.	Release Date
NJ101-[][][][]	Ver.1.64.04 or higher	26424 or later	April 26, 2024
NJ301-[][][][]	Ver.1.64.04 or higher	26424 or later	April 26, 2024
NJ501-1[]0[]	Ver.1.64.04 or higher	26424 or later	April 26, 2024
NJ501-1[]2[]	Ver.1.64.04 or higher	26424 or later	April 26, 2024
NJ501-1340	Ver.1.64.04 or higher	26424 or later	April 26, 2024
NJ501-4[][][]	Ver.1.64.04 or higher	26424 or later	April 26, 2024
NJ501-5300	Ver.1.64.04 or higher	26424 or later	April 26, 2024
NJ501-R[][][]	Ver.1.64.04 or higher	26424 or later	April 26, 2024

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.1.64.04 or higher	26424 or later	April 26, 2024
NX1P2-[][][][][][]	Ver.1.64.04 or higher	26424 or later	April 26, 2024
NX1P2-[][][][][][]1	Ver.1.64.04 or higher	26424 or later	April 26, 2024
NX502-[][][][]	Ver.1.66.01 or higher	26424 or later	April 26, 2024
NX701-[][][][]	Ver.1.35.04 or higher	26424 or later	April 26, 2024
NX-EIP201	Ver.1.01.00 or higher	26424 or later	April 26, 2024

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. 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.

C09-27-01B

- 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.

■Contact information
Please contact our sales office or distributors.
https://www.ia.omron.com/global_network/index.html
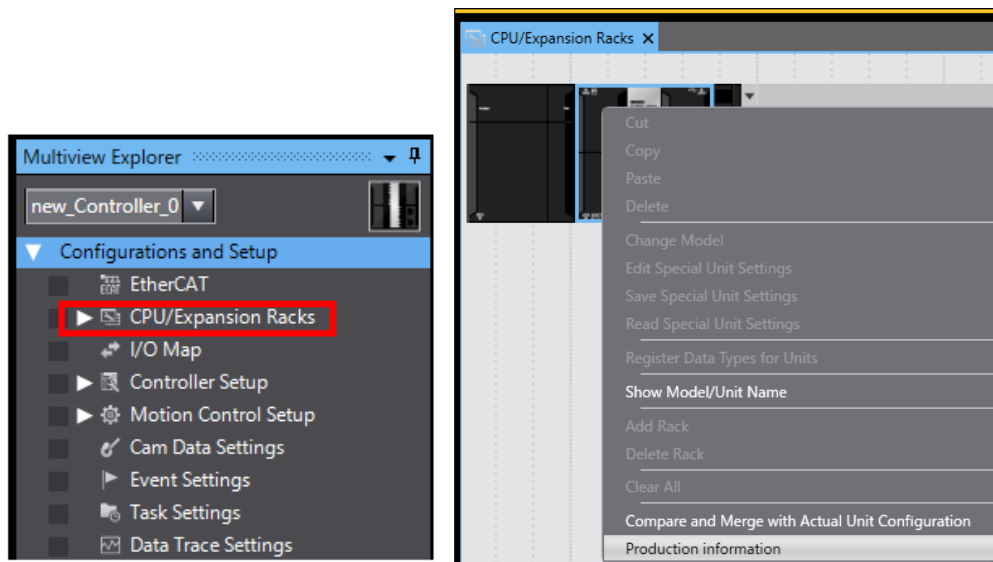
■Update history
- May 27, 2024: New Release

C09-27-01B

Appendix How to check the product version

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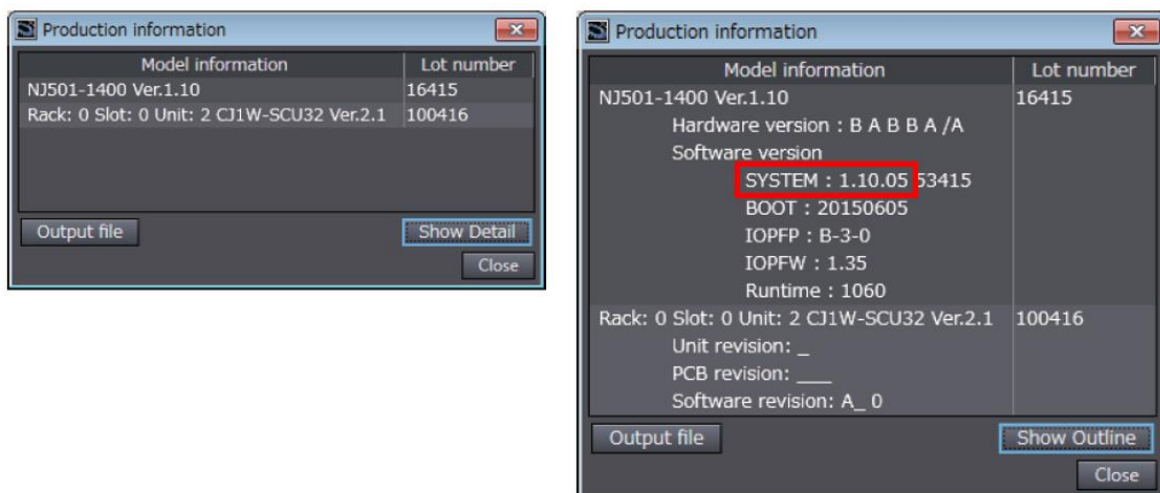
For NJ-series

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**.
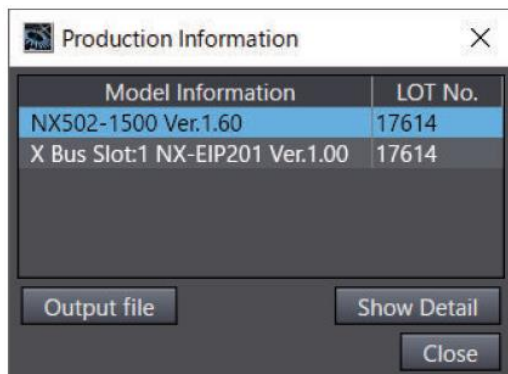

Click the **Show Detail** Button at the lower right of the Production Information Dialog Box.

The figure below shows Ver.1.10.05.

C09-27-01B

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).

C09-27-01B