Insufficient Verification of Data Authenticity vulnerability in NJ/NX-series Machine Automation Controllers

Release date: May 27, 2024
OMRON Corporation

■Overview

Insufficient Verification of Data Authenticity (CWE-345) vulnerability exists in the NJ/NX-series Machine Automation Controllers. Due to this vulnerability, the controller product may not be able to detect that the user program within the product has been tampered with.

The products and versions affected by this vulnerability, countermeasures, 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. 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, all versions
- Machine Automation Controller NX-series, all versions

■Description

Due to the Insufficient Verification of Data Authenticity (CWE-345) vulnerability which exists in the NJ/NX-series Machine Automation Controllers, the products may not be able to detect that the user program within the product has been tampered with.

■CVSS Scores

Insufficient Verification of Data Authenticity (CWE-345)
CVE-2024- 33687
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N Base Score 4.8

■Countermeasures

The countermeasures against the vulnerability can be taken by using the followings.

- User Program Transfer with No Restoration Information
- Normally, when you transfer the user program from the Sysmac Studio to the CPU Unit, information is transferred to restore it. This function does not transfer information for

restoration. That makes it impossible to tamper with the user program.

Please refer to the “User Program Transfer with No Restoration Information” in the manual to know details.

- NJ/NX-series CPU unit Software User’s Manual (W501)

■ 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.

■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

- May 27, 2024: New Release