Pass Traversal Vulnerability in Automation Software Sysmac Studio and NX-IO Configurator

Release date: September 19, 2023
OMRON Corporation

■Overview

Path Traversal (CWE-22) vulnerability exist in the Automation Software Sysmac Studio. An Attacker may use this vulnerability to create a file in any path on a computer.

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.

Product series	Model	Version
Automation Software Sysmac Studio	SYSMAC-SE2[][][]	Ver.1.54 or lower
NX-IO Configurator	Included in CX-One CXONE-AL[][]D-V4	Ver.1.22 or lower

Refer to the following manuals for how to check the target product version.

- Sysmac Studio Version 1 Operation Manual (W504)
- NX-IO Configurator Operation Manual (W585)

■Description

Automation Software Sysmac Studio and NX-IO Configurator have the vulnerability known as path traversal (CWE-22), which allows attackers to create a file in any location on a computer.

■Potential threats and impacts

An attacker may be able to put an attack file in a target computer to manipulate it illegally.

■CVSS Scores

Path Traversal (CWE-22)

CVE-2018-1002205

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N Base Score 5.5

■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.
   - 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.

■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.

Product series	Model	Version	Release date
Automation Software Sysmac Studio	SYSMAC-SE2[][][]	Ver.1.55 or higher	July 18, 2023
NX-IO Configurator	Included in CX-One CXONE-AL[][]D-V4	Ver.1.23 or higher	April 24, 2023

For information on how to obtain and update the countermeasure version of the product, please contact our sales office or distributors. You can update the Sysmac Studio to the latest versions using the installed Omron Automation Software Auto-Update tool.

■Contact information

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

■Acknowledgments

Reid Wightman of Dragos reported this vulnerability through CISA.
Michael Heinzl reported this vulnerability through JPCERT/CC.
Thanks to Reid Wightman and Michael Heinzl for finding and reporting it.

■Update history

- September 19, 2023: New Release