Incorrect Authorization (CWE-863) vulnerability in Sysmac Studio Software

Release date: November 1st, 2024
OMRON Corporation

■ Overview

Incorrect Authorization (CWE-863) vulnerability exists in Sysmac Studio Software. An attacker may use the vulnerability to illegally access programs protected by Data Protection function.

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.

Sysmac Studio Software

Model	Version
SYSMAC-SE2[][][]	All

Refer to “Displaying and Registering Licenses” section in the above manual to check the product version.

- Sysmac Studio Version 1 Operation Manual (W504)

■ Description

Due to Incorrect Authorization (CWE-863) vulnerability which exists in Sysmac Studio Software, programs protected by Data Protection function may be illegally accessed.

■ CVSS Scores

Incorrect Authorization (CWE-863)

CVE-2024-49501

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N Base Score 5.7

■Countermeasures

The countermeasures against the vulnerability can be implemented by protecting assets using Library Without Source Code, which is more strongly protective than Data Protection. Where the countermeasures against the vulnerability are needed, please follow the steps below to use Library Without Source Code.

1. Update the product to the security enhanced countermeasure version

   Sysmac Studio Software

Model	Version	Release date
SYSMAC-SE2[][][]	Ver.1.60 or later	October 16th, 2024

   You can update to the latest versions using the installed Omron Automation Software AutoUpdate tool.

2. Store the program that you wish to protect into Library Without Source Code

   For how to use Library Without Source Code, see the Sysmac Studio Version 1 Operation Manual (W504).

■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.

■Update history

- November 1st, 2024: New Release