

Free of Pointer not at Start of Buffer vulnerability in Common Modules of Sysmac Studio and CX-One

Release date: April 22, 2024
OMRON Corporation

■ Overview

Free of Pointer not at Start of Buffer vulnerability (CWE-761) was found in common modules of Sysmac Studio and CX-One. Attackers may be able to execute arbitrary codes on a computer by abusing this vulnerability.

The products and versions affected by this vulnerability, 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. 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.

Product series	Model	Version
CX-One	CX-One CXONE-AL[[]]D-V4	The version which was installed with a DVD ver. 4.61.1 or lower, and was updated through CX-One V4 auto-update in January 2024 or prior.
Sysmac Studio	SYSMAC-SE2[[]][[]]	The version which was installed with a DVD ver. 1.56 or lower, and was updated through Sysmac Studio V1 auto-update in January 2024 or prior.

Refer to the appendix for how to check the target product version.

■ Description

Common modules of Sysmac Studio and CX-One have vulnerability known as Free of Pointer not at Start of Buffer (CWE-761), which allow attackers to execute arbitrary codes on a computer.

■ CVSS Scores

Free of Pointer not at Start of Buffer vulnerability (CWE-761)

CVE-2024-31413

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H Base Score: 7.8

■ Countermeasure

Update Common Components of your Sysmac Studio or CX-One applying the countermeasure version to fix the vulnerability. The countermeasure version and respective release date for each product is shown in the table below.

Product series	Model	Version to be released	Scheduled release
CX-One	CX-One CXONE-AL[[[D-V4	CX-One Version 4 auto-update (April 2024) or later	April 22, 2024
Sysmac Studio	SYSMAC-SE2[[[[]	Sysmac Studio Version 1 auto-update (April 2024) or later (Ver. 1.58 or higher)	April 22, 2024

For information on how to obtain and update the countermeasure version of the product, please contact our sales representative or distributor. You can update CX-One to the latest versions using the installed Omron Automation Software AutoUpdate tool.

■ 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

Michael Heinzl reported this vulnerability through JPCERT/CC.

Thanks to Michael Heinzl for finding and reporting the vulnerability.

■ Update history

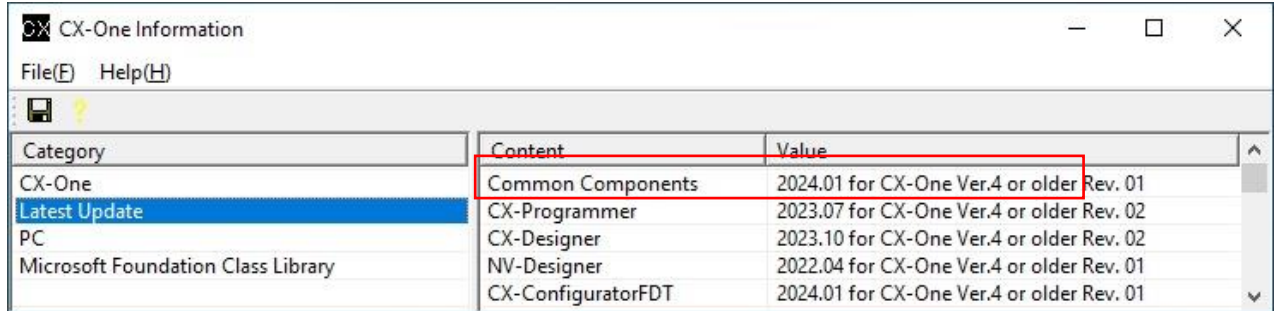
- April 22, 2024: New Release

Appendix: How to check the product version

CX-One

Run CX-One Information from the start menu: [Omron] – [CX-One] – [CX-One Information] and then, see the Value column of Common Components.

The following shows CX-One Version 4 auto-update (January 2024) has been installed.



Category	Content	Value
CX-One	Common Components	2024.01 for CX-One Ver.4 or older Rev. 01
Latest Update	CX-Programmer	2023.07 for CX-One Ver.4 or older Rev. 02
PC	CX-Designer	2023.10 for CX-One Ver.4 or older Rev. 02
Microsoft Foundation Class Library	NV-Designer	2022.04 for CX-One Ver.4 or older Rev. 01
	CX-ConfiguratorFDT	2024.01 for CX-One Ver.4 or older Rev. 01

Sysmac Studio

Click [License] on the Sysmac Studio start page and then, see Module version.

