Out-of-bounds Read vulnerability in CX-Programmer

Release date: February 17, 2025
Last modified on March 10, 2025
OMRON Corporation

■ Overview

Out-of-bounds Read vulnerability (CWE-125) was found in CX-Programmer. Attackers may be able to read sensitive information or cause an application crash by abusing this vulnerability.

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.

FA Integrated Tool Package CX-One

Product	Model	Version
CX-Programmer	CX-One Ver.4 (CXONE-AL[][]D-V4) * CX-Programmer is included in CX-One.	Ver.9.83 or lower

Refer to “About CX-Programmer” in “Technical Specifications” of the manual below to check the product version.

- CX-Programmer Ver.9.[] Operation Manual (W446)

■ Description

CX-Programmer has the vulnerability known as Out-of-bounds Read (CWE-125), which allows attackers to read sensitive information in the CX-Programmer or cause the CX-Programmer to crash.

However, the CX-Programmer installed computer and the CX-Programmer connected PLC are not affected.

■CWE,CVE,CVSS Scores

Out-of-bounds Read (CWE-125)

CVE-2025-0591

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

■Countermeasures

Update your CX-Programmer to the countermeasure version to fix the vulnerability. The countermeasure version and respective release date for each product is shown in the table below.

FA Integrated Tool Package CX-One

Product	Model	Version	Release Date
CX-Programmer	CX-One Ver.4 (CXONE-AL[][]D-V4) * CX-Programmer is included in CX-One.	Ver.9.84 or higher	January 8, 2025

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 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.

■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

- February 17, 2025: New Release
- March 10, 2025: Update the Description