Out-of-bounds Read, Use After Free and

Heap-based Buffer Overflow Vulnerabilities

in CX-Programmer

Release date: August 1, 2023

OMRON Corporation

■Overview

An out-of-bounds read memory corruption vulnerability (CWE-125), a use after freed memory vulnerability (CWE-416) and a heap-based buffer overflow vulnerability (CWE-122) have been found in CX-Programmer. Malicious users may exploit these vulnerabilities and execute arbitrary codes.

The affected versions, defensive measures, and solution are described below. Please take the following defensive measures to minimize the risk of exploitation of these vulnerabilities. We have also released a security-enhanced version to ensure reliability.

■Affected Products

The following versions are affected by these vulnerabilities.

Product Name	Type	Version
CX-Programmer	Included in CX-One CXONE-AL[][]D-V4	V9.80 or lower

Please refer to the following manual for how to check the version of your CX-Programmer.

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

■Vulnerability Description

CX-Programmer contains an out-of-bounds read memory corruption vulnerability (CWE-125), a use after freed memory vulnerability (CWE-416) and a heap-based buffer overflow vulnerability (CWE-122)

■Impact

Malicious users may exploit these vulnerabilities and execute arbitrary codes.

■CVSS Score

Out-of-bounds Read (CWE-125)

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

Heap-based Buffer Overflow (CWE-122)

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

Use After Free (CWE-416)

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

■Mitigations and Protections

OMRON recommends that customers take the following mitigation measures to minimize the risk of exploitation of these vulnerabilities.

1. Anti-virus measure

Installation of the latest commercial-quality anti-virus software in your computer that is connected to the control systems

2. Prevention of Unauthorized Access

・Keeping the minimal connection of the control systems and equipment to the network and forbiting access from unreliable devices

・Isolation from the IT network via a firewall (Disabling unused communication ports, Limiting the number of communication hosts)

・Use of a virtual private network (VPN) when remotely accessing to the control systems

・Strong passwords and frequent changes to them

・Adoption of physical security control that allows only an authorized person to access the control systems and equipment

・Virus check for external storage devices such as USBs before using them in the control systems and equipment

・Applying multi-factor authentication to the control systems and equipment

3. Protection of Input and Output Data

Assuring backup and range check validity in case of unintentional modification of data input to and output from the control systems and equipment

4. Restoration of Lost Data

Periodic backup and maintenance of setting data to prevent loss of data

■Countermeasures

Please update your CX-Programmer to the security-enhanced version.

The version and release date are as follows.

Product Name	Type	Version	Release Date
CX-Programmer	Included in CX-One CXONE-AL[][]D-V4	V9.81 or higher	July 3, 2023

For the security-enhanced version and how to install it, please contact your OMRON representative.

■Contact

Contact your OMRON distributer or your OMRON representative.

Japan: https://www.fa.omron.co.jp/sales/local/

Overseas: https://www.ia.omron.com/global_network/index.html

■Acknowledgments

These vulnerabilities were discovered and reported by Mr. Michael Heinzl via JPCERT/CC.

We thank Mr. Michael Heinzl for this.

■Update History

August 1, 2023: New Release