Vulnerability Report on Improper Restriction of XML External Entity Reference in CX-Designer

Release date: October 23, 2023
OMRON Corporation

■Overview

We found a vulnerability Improper Restriction of XML External Entity Reference (CWE-611) in CX-Designer. Attackers may be able to abuse this vulnerability to disclose confidential data 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
CX-Designer	Included in CX-One CXONE-AL[][]D-V4	Ver. 3.740 and prior

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

・ CX-Designer Ver.3.[] USER'S MANUAL (V099-E1-12)

■Description

CX-Designer has the vulnerability known as Improper Restriction of XML External Entity Reference (CWE-611).

■Potential threats and impacts

Attackers may be able to disclose confidential data on a computer.

■CVSS Scores

Restriction of XML External Entity Reference (CWE-611)
CVE-2023-43624
CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N Base Score 5.5

■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
CX-Designer	Included in CX-One CXONE-AL[][]D-V4	Ver. 3.750 or later	October 2, 2023

For information on how to obtain and update the firmware for the countermeasure version of the product, please contact our sales office or distributors.

■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

■Acknowledgments

We are grateful for the commitment of Mr. Michael Heinzl to finding and reporting this vulnerability through JPCERT/CC.

■Update history

- October 23, 2023: New Release