Support tool CX-Drive for inverter/servo heap-based buffer overflow vulnerability

Published 2023 April 24
Last modified on August 1, 2023
OMRON Corporation

■Overview

CX-Drive, a support tool for inverters/servos, was found to contain a heap-based buffer overflow vulnerability (CWE-122). A local attacker can exploit this issue to disclose information and execute arbitrary code on an affected CX-Drive installation.

Exploitation of this vulnerability requires user interaction, which is a requirement that a user open a malicious SDD file.

The affected products, versions, mitigations and workarounds are listed below. By implementing mitigations and workarounds recommended by the Company, the risk of exploitation of this vulnerability can be minimized.

■Affected products

The types and versions of products affected by this vulnerability are as follows.

series	format	Target version
CX-Drive	All formats	All versions

For how to check the target product version, refer to the following manual.

・CX-Drive Operation User's Manual (SBCE-375)

■CVSS Score

Heap-based buffer overflow (CWE-122)

CVE-2023-27385

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

■Mitigations and Workarounds

In order to minimize the risk of exploitation of this vulnerability, we recommend that you take the following mitigations and workarounds measures.

1. Antivirus Protection

・Installation and maintenance of the latest commercial-quality anti-virus software on PCs connected to the control system

・Do not execute suspicious project files

2. Prevention of unauthorized access

• Minimize network connectivity of control systems and equipment and prohibit access from untrusted devices

・Isolation from the IT network by introducing firewalls (blocking unused communication ports, restricting communication hosts)

・If remote access to control systems and equipment is required, use a virtual private network (VPN)

・Adopt strong passwords and change them frequently

・Introduction of physical controls that allow only authorized persons to access control systems and equipment.

• Pre-virus scanning when using external storage devices such as USB sticks in control systems and devices

・Introduction of multi-factor authentication for remote access to control systems and equipment

3. Securing data input and output

・Validation of backup and range checks in preparation for unintentional modification of input/output data to control systems and devices

4. Recover lost data

・Regular backup and maintenance of configuration data as a measure against data loss

5. Adoption of new software tools and controllers

・Automation software Sysmac Studio

・Controller NJ/NX/NY Series

■Acknowledgments

Michael Heinzl reported this vulnerability through JPCERT/CC.

Thanks to Michael Heinzl for finding and reporting vulnerabilities.

■Update History

April 24, 2023: New Release

August 1, 2023: Added Affected products version.