TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerability in SICK Flexi Soft Designer & Safety Designer

Document ID:	SCA-2022-0010
Publication Date:	2022-05-16
CVSSv3 Base Score:	8.6
CVSS Vector String:	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H
CWE:	Deserialization of untrusted data (CWE-502)
Version:	V1.0

SUMMARY

A vulnerability in a .NET framework class used by Safety Designer / Flexi Soft Designer allows an attacker to craft malicious project files. Opening/importing such a malicious project file would execute arbitrary code with the privileges of the current user when opened or imported by a Safety Designer / Flexi Soft Designer. This compromises confidentiality, integrity and availability.
For the attack to succeed, a user must manually open a malicious project file.

The vulnerability was found in internal code review. Currently SICK is not aware of any public exploits targeting this vulnerability.

AFFECTED PRODUCTS

Product	Version	Remediation available
SICK Flexi Soft Designer	≤ 1.9.4 SP1	Yes, update to newest version
SICK Safety Designer	≤ 1.11.0	Yes, update to newest version

SOLUTION

The recommended solution is to update Safety Designer / Flexi Soft Designer to the latest version as soon as possible. Note that projects created with Safety Designer 1.12.0 cannot be loaded in earlier versions.

If you cannot update to an unaffected version, please make sure that you:

- Only open/import project files from trusted sources
- Do not run Safety Designer / Flexi Soft Designer under a windows account with elevated privileges

General Security Practices

As general security measures, SICK recommends to minimize network exposure of the devices, restrict network access and follow recommended security practices in order to run the devices in a protected IT environment.

Additional information on Industrial Security can be found at:
http://ics-cert.us-cert.gov/content/recommended-practices

VULNERABILITY CLASSIFICATION

SICK performs vulnerability classification by using the CVSS scoring system (CVSS v3.1). The environmental score is dependent on the customer's environment and can affect the overall CVSS score. SICK recommends that customers individually evaluate the environmental score to achieve final scoring.

RESOURCES

SICK PSIRT Security Advisories
https://sick.com/psirt

SICK Operating Guidelines
https://cdn.sick.com/media/docs/1/11/411/Special_information_CYBERSECURITY_BY_SICK_en_IM0084411.PDF

HISTORY

Version	Release Date	Comment
V1	2022-05-16	Initial Release