SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerability in SICK Flexi Soft Designer & Safety Designer

Document ID:	SCA-2022-0010
Publication Date:	2022-07-19
CVE Identifiers:	CVE-2022-27579, CVE-2022-27580
Version:	V2.0

Summary

A deserialization vulnerability in a .NET framework class used by both SICK Flexi Soft Designer and SICK Safety Designer allows an attacker to create malicious project files.

Affected Products

Product	Model Numbers	Affected by
SICK Flexi Soft Designer	<= 1.9.4 SP1	CVE-2022-27579 Status: Last Affected Remediation: Yes (vendor fix)
SICK Safety Designer	<= 1.11.0	CVE-2022-27580 Status: Last Affected Remediation: Yes (vendor fix)

Vulnerability Overview

CVE-2022-27579 Deserialization of Untrusted Data

A deserialization vulnerability in a .NET framework class used and not properly checked by Flexi Soft Designer in all versions up to and including 1.9.4 SP1 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 the Flexi Soft Designer. This compromises confidentiality integrity and availability.For the attack to succeed a user must manually open a malicious project file.

CVE-2022-27579 has been assigned to this vulnerability.
CVSSv3.1 base score: 8.6
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

References:
Microsoft Security Guide: https://docs.microsoft.com/en-us/dotnet/standard/serialization/binaryformatter-security-guide

CVE-2022-27580 Deserialization of Untrusted Data

A deserialization vulnerability in a .NET framework class used and not properly checked by Safety Designer all versions up to and including 1.11.0 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 the Safety Designer. This compromises confidentiality integrity and availability.For the attack to succeed a user must manually open a malicious project file.

CVE-2022-27580 has been assigned to this vulnerability.
CVSSv3.1 base score: 8.6
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

References:
Microsoft Security Guide: https://docs.microsoft.com/en-us/dotnet/standard/serialization/binaryformatter-security-guide

Remediations

Vendor Fix for CVE-2022-27579

Valid for: SICK Flexi Soft Designer

Details: The recommended solution is to update Flexi Soft Designer to the latest version as soon as possible.
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

Vendor Fix for CVE-2022-27580

Valid for: SICK Safety Designer

Details: The recommended solution is to update Safety 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.

Product Glossary

SICK Flexi Soft Designer	The strength of the Flexi Soft Designer configuration tool is that it enables users to create easy and straightforward configurations for the Flexi Soft safety controller. Only three steps are needed (hardware configuration, logic creation and transfer, and verification) to produce the configuration. The easy-to-follow user guide in the configuration tool provides information on the modules and elements, as well as a graphical wiring diagram for quick commissioning, plus full documentation. Configuring a Flexi-Link project with the Flexi Soft Designer is also easy. Each station is configured separately; however, the actual Flexi-Link project is saved in a single project file.
SICK Safety Designer	Safety Designer is the SICK configuration software for safety solutions.

History

Version	Release Date	Comment
V1.0	2022-05-16	Initial Release
V2.0	2022-07-19	Assigned CVEs