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:	3

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.

List of Products

Product	Affected by
SICK Flexi Soft Designer <=1.9.4 SP1	CVE-2022-27579 Status: Known Affected Remediation: Vendor fix
SICK Safety Designer <=1.11.0	CVE-2022-27580 Status: Known Affected Remediation: Vendor fix

Vulnerability Overview

CVE-2022-27579 Deserialization of Untrusted Data

Description: 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
CWE identifier: CWE-502 (Deserialization of Untrusted Data)

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

CVE-2022-27580 Deserialization of Untrusted Data

Description: 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
CWE identifier: CWE-502 (Deserialization of Untrusted Data)

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

Remediations

Vendor Fix for CVE-2022-27579

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

Valid for:

- SICK Flexi Soft Designer <=1.9.4 SP1

Vendor Fix for CVE-2022-27580

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

Valid for:

- SICK Safety Designer <=1.11.0

General Security Practices

General Security Measures

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.

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

ICS-CERT recommended practices on Industrial Security:
http://ics-cert.us-cert.gov/content/recommended-practices

CVSS v3.1 Calculator:
https://www.first.org/cvss/calculator/3.1

Additional Product Information

SICK Flexi Soft Designer <=1.9.4 SP1	Product on sick.com: https://www.sick.com/de/de/p/p674217
SICK Safety Designer <=1.11.0	Product on sick.com: https://www.sick.com/de/de/p/p674218

History

Version	Release Date	Comment
1	2022-05-16	Initial Release
2	2022-07-19	Assigned CVEs
3	2023-02-10	Updated Advisory (only visual changes)