Security Advisory
SafeLogic Designer vulnerabilities

1 Advisory Information

Advisory ID: BOSCH-SA-463993
CVE Numbers and CVSS v3.1 Scores:

- CVE-2022-27579
  - Base Score: 7.8 (High)
- CVE-2022-27580
  - Base Score: 7.8 (High)

Published: 11 Aug 2022
Last Updated: 11 Aug 2022

2 Summary

The SafeLogic Designer from Bosch Rexroth contains technology from SICK AG. The manufacturer has published a security bulletin regarding a vulnerability in the .NET framework [1].

A vulnerability in a .NET framework class used by SafeLogic 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 SafeLogic Designer. This compromises confidentiality, integrity and availability.
For the attack to succeed, a user must manually open a malicious project file.

All versions of SafeLogic Designer prior to 1.8.0.763_SP1 are affected by the vulnerability.

3 Affected Products

- SafeLogic Designer < 1.8.0.763_SP1

4 Solution

The recommended solution is to update SafeLogic Designer to the latest version as soon as possible.

4.1 Mitigation

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

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

4.2 Compensatory Measures

Compensatory measures are recommended which mitigate the risk. Always define such compensatory measures individually, in the context of the operational environment. Some measures are described in the “Security Guideline Electric Drives and Controls”, for example the network segmentation. In general, it is mandatory to implement the measures described in the “Security Guideline Electric Drives and Controls” [2].

5 Vulnerability Details

5.1 CVE-2022-27579

CVE 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.

- Problem Type:
  - CWE-502
- CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
  - Base Score: 7.8 (High)

5.2 CVE-2022-27580

CVE 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.

- Problem Type:
  - CWE-502
- CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
  - Base Score: 7.8 (High)

6 Additional Resources

[1] SICK Advisory SCA-2022-0010:
https://www.sick.com/medias/sca-2022-0010.pdf?context=bWFzdGVyfGNvbnRlbnR8OTU3OTh8YXBwbGljYXRpb24vcGRmfGNvbnRlbnQvaDI2L2g5My8xMjgzMTU0NDU0MTIxNC5wZGZ8ZDJmZGZkOGQ3NzFlYTNiODA3NDUxMWJiOTkyNjhiYTExMmZlN2E2ZjJiNWJlODk0N2I4NmFmODFkOWI3YTc1OQ

[2] Bosch Rexroth Security Guideline Electric Drives and Controls:
https://www.boschrexroth.com/various/utilities/mediadirectory/download/index.jsp?object_nr=R911342562

7 Revision History

11 Aug 2022: Initial Publication