SSA-932528: Multiple File Parsing Vulnerabilities in Solid Edge

Publication Date:	2023-05-09
Last Update:	2023-08-08
Current Version:	V1.1
CVSS v3.1 Base Score:	7.8

SUMMARY

Solid Edge is affected by multiple memory corruption vulnerabilities that could be triggered when the application reads specially crafted files in various formats such as DWG, IFC, OBJ or STP format. If a user is tricked to open a malicious file with the affected application, an attacker could leverage the vulnerability to crash the application or execute arbitrary code.

Siemens has released several updates for Solid Edge SE2023 and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Solid Edge SE2023: All versions < V223.0 Update 3 only affected by CVE-2023-30985, CVE-2023-30986	Update to V223.0 Update 3 or later version https://support.sw.siemens.com/ See recommendations from section Workarounds and Mitigations
Solid Edge SE2023: All versions < V223.0 Update 2	Update to V223.0 Update 2 or later version https://support.sw.siemens.com/ See recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Avoid to open untrusted files from unknown sources in Solid Edge

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals. Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

Solid Edge is a portfolio of software tools that addresses various product development processes: 3D design, simulation, manufacturing and design management.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2023-0973

STEPTools v18SP1 ifcmesh library (v18.1) is affected due to a null pointer dereference, which could allow an attacker to deny application usage when reading a specially constructed file, resulting in an application crash. (ZDI-CAN-19429)

CVSS v3.1 Base Score	2.2
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2023-30985

Affected applications contain an out of bounds read past the end of an allocated buffer while parsing a specially crafted OBJ file. This vulnerability could allow an attacker to disclose sensitive information. (ZDI-CAN-19426)

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2023-30986

Affected applications contain a memory corruption vulnerability while parsing specially crafted STP files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19561)

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2023-39549

The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted DWG file. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-19562)

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:T/RC:C
CWE	CWE-416: Use After Free

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Trend Micro Zero Day Initiative for coordinated disclosure

ADDITIONAL INFORMATION

This advisory covers a security vulnerability (CVE-2023-0973) in STEPTools ifcmesh library from Step Tools, Inc [1].

[1] ICSA-23-068-04: https://www.cisa.gov/news-events/ics-advisories/icsa-23-068-04

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2023-05-09):	Publication Date
V1.1 (2023-08-08):	Added CVE-2023-39549 fixed in Solid Edge 223.0 Update 2

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.