

## **SSA-382651: File Parsing Vulnerability in Solid Edge before V223.0.11**

Publication Date: 2024-03-12  
Last Update: 2024-03-12  
Current Version: V1.0  
CVSS v3.1 Base Score: 7.8  
CVSS v4.0 Base Score: 7.3

### **SUMMARY**

Solid Edge is affected by an out of bounds read vulnerability that could be triggered when the application reads files that contains XT parts. If a user is tricked to open a malicious file with the affected applications, an attacker could leverage the vulnerability to perform remote code execution in the context of the current process.

Siemens has released a new version for Solid Edge and recommends to update to the latest version.

### **AFFECTED PRODUCTS AND SOLUTION**

<b>Affected Product and Versions</b>	<b>Remediation</b>
Solid Edge: All versions < V223.0.11 affected by <a href="#">all CVEs</a>	Update to V223.0.11 or later version <a href="https://solidedge.siemens.com/">https://solidedge.siemens.com/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

### **WORKAROUNDS AND MITIGATIONS**

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

- Do not open untrusted files containing XT parts 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 DESCRIPTION**

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

### **Vulnerability CVE-2023-49125**

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted files containing XT format. This could allow an attacker to execute code in the context of the current process.

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
CVSS v4.0 Base Score	7.3
CVSS Vector	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-125: Out-of-bounds Read

## **ACKNOWLEDGMENTS**

Siemens thanks the following party for its efforts:

- Michael Heinzl for coordinated disclosure of CVE-2023-49125

## **ADDITIONAL INFORMATION**

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 (2024-03-12): Publication Date

## **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](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.