SSA-797296: XT File Parsing Vulnerability in Parasolid

Publication Date:	2024-02-13
Last Update:	2024-02-13
Current Version:	V1.0
CVSS v3.1 Base Score:	7.8
CVSS v4.0 Base Score:	7.3

SUMMARY

Parasolid is affected by out of bounds read and null pointer dereference vulnerabilities that could be triggered when the application reads files in XT format. 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 new versions for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Parasolid V35.0: All versions < V35.0.263 affected by CVE-2023-49125	Update to V35.0.263 or later version https://support.sw.siemens.com/en-US/product/258316782/ See further recommendations from section Workarounds and Mitigations
Parasolid V35.0: All versions < V35.0.251 affected by CVE-2024-22043	Update to V35.0.251 or later version https://support.sw.siemens.com/en-US/product/258316782/ See further recommendations from section Workarounds and Mitigations
Parasolid V35.1: All versions < V35.1.252 affected by CVE-2023-49125	Update to V35.1.252 or later version https://support.sw.siemens.com/en-US/product/258316782/ See further recommendations from section Workarounds and Mitigations
Parasolid V35.1: All versions < V35.1.170 affected by CVE-2024-22043	Update to V35.1.170 or later version https://support.sw.siemens.com/en-US/product/258316782/ See further recommendations from section Workarounds and Mitigations
Parasolid V36.0: All versions < V36.0.198 affected by CVE-2023-49125	Update to V36.0.198 or later version https://support.sw.siemens.com/en-US/product/258316782/ See further 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:

- Do not open untrusted XT files in Parasolid

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

Parasolid is a 3D geometric modeling tool that supports various techniques, including solid modeling, direct editing, and free-form surface/sheet modeling.

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

Vulnerability CVE-2024-22043

The affected applications contain a null pointer dereference vulnerability while parsing specially crafted XT files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CVSS v4.0 Base Score	4.8
CVSS Vector	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N
CWE	CWE-476: NULL Pointer Dereference

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Michael Heinzl for coordinated disclosure of CVE-2023-49125
- Jin Huang from ADLab of Venustech for reporting the vulnerability CVE-2024-22043

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 (2024-02-13):	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, 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.