SSA-407785: Multiple X_T File Parsing Vulnerabilities in Parasolid and Teamcenter Visualization

Publication Date: 2023-08-08
Last Update: 2024-08-13
Current Version: V1.3
CVSS v3.1 Base Score: 7.8
CVSS v4.0 Base Score: 7.3

SUMMARY

Parasolid and Teamcenter Visualization are affected by memory corruption vulnerabilities that could be triggered when the application reads files in X_T 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 or denial of service in the context of the current process.

Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens recommends specific countermeasures for products where fixes are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Parasolid V34.1: All versions < V34.1.258 affected by all CVEs	Update to V34.1.258 or later version https://support.sw.siemens.com/product/258316782/ See further recommendations from section Workarounds and Mitigations
Parasolid V35.0: All versions < V35.0.254 affected by all CVEs	Update to V35.0.254 or later version https://support.sw.siemens.com/product/258316782/ See further recommendations from section Workarounds and Mitigations
Parasolid V35.1:	See below https://support.sw.siemens.com/product/258316782/ See further recommendations from section Workarounds and Mitigations
Parasolid V35.1: All versions < V35.1.171 affected by CVE-2023-38524, CVE-2023-38525, CVE-2023-38526, CVE-2023-38530, CVE-2023-38532	Update to V35.1.171 or later version https://support.sw.siemens.com/product/258316782/ See further recommendations from section Workarounds and Mitigations
Parasolid V35.1: All versions < V35.1.197 affected by CVE-2023-38528	Update to V35.1.197 or later version https://support.sw.siemens.com/product/258316782/ See further recommendations from section Workarounds and Mitigations

Parasolid V35.1: All versions < V35.1.184 affected by CVE-2023-38528, CVE-2023-38529, CVE-2023-38531	Update to V35.1.184 or later version https://support.sw.siemens.com/product/258316782/ See further recommendations from section Workarounds and Mitigations
Teamcenter Visualization V14.1:	See below See further recommendations from section Workarounds and Mitigations
Teamcenter Visualization V14.1: All versions < V14.1.0.11 affected by CVE-2023-38524, CVE-2023-38525, CVE-2023-38526, CVE-2023-38528, CVE-2023-38530, CVE-2023-38532	Update to V14.1.0.11 or later version https://support.sw.siemens.com/product/229029598/ See further recommendations from section Workarounds and Mitigations
Teamcenter Visualization V14.1: All versions affected by CVE-2023-38527, CVE-2023-38529, CVE-2023-38531	Currently no fix is planned See recommendations from section Workarounds and Mitigations
Teamcenter Visualization V14.2:	See below https://support.sw.siemens.com/product/229029598/ See further recommendations from section Workarounds and Mitigations
Teamcenter Visualization V14.2: All versions < V14.2.0.6 affected by CVE-2023-38524, CVE-2023-38525, CVE-2023-38526, CVE-2023-38528, CVE-2023-38530, CVE-2023-38532	Update to V14.2.0.6 or later version https://support.sw.siemens.com/product/229029598/ See further recommendations from section Workarounds and Mitigations
Teamcenter Visualization V14.2: All versions < V14.2.0.12 affected by CVE-2023-38527, CVE-2023-38529, CVE-2023-38531	Update to V14.2.0.12 or later version https://support.sw.siemens.com/product/229029598/ See further recommendations from section Workarounds and Mitigations
Teamcenter Visualization V14.3:	See below https://support.sw.siemens.com/product/229029598/ See further recommendations from section Workarounds and Mitigations
Teamcenter Visualization V14.3: All versions < V14.3.0.3 affected by CVE-2023-38524, CVE-2023-38525, CVE-2023-38526, CVE-2023-38528, CVE-2023-38530, CVE-2023-38532	Update to V14.3.0.3 or later version https://support.sw.siemens.com/product/229029598/ See further recommendations from section Workarounds and Mitigations

Teamcenter Visualization V14.3: All versions < V14.3.0.9 affected by CVE-2023-38527, CVE-2023-38529, CVE-2023-38531	Update to V14.3.0.9 or later version https://support.sw.siemens.com/product/229029598/ See further recommendations from section Workarounds and Mitigations
Teamcenter Visualization V2312: All versions < V2312.0004 affected by CVE-2023-38527, CVE-2023-38529, CVE-2023-38531	Update to V2312.0004 or later version https://support.sw.siemens.com/product/229029598/ 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 or Teamcenter Visualization

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.

Teamcenter Visualization software enables enterprises to enhance their product lifecycle management (PLM) environment with a comprehensive family of visualization solutions. The software enables enterprise users to access documents, 2D drawings and 3D models in a single environment.

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-2023-38524

The affected applications contain null pointer dereference while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.

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	2.0
CVSS Vector	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:P/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2023-38525

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. 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-2023-38526

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. 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-2023-38527

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. 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-2023-38528

The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted X_T file. 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-787: Out-of-bounds Write

Vulnerability CVE-2023-38529

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. 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-2023-38530

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. 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-2023-38531

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. 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-2023-38532

The affected application contains a stack exhaustion vulnerability while parsing a specially crafted X_T file. This could allow an attacker to cause 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-770: Allocation of Resources Without Limits or Throttling

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Jin Huang from ADLab of Venustech for reporting the vulnerabilities

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 (2023-08-08): Publication Date
V1.1 (2023-11-14): Added fixes for Teamcenter Visualization V14.1 and Teamcenter Visualization V14.3
V1.2 (2024-06-11): Corrected error regarding fix information for CVE-2023-38527, CVE-2023-38529 and CVE-2023-38531 for Teamcenter Visualization V14.1, Teamcenter Visualization V14.2 and Teamcenter Visualization V14.3 and added Teamcenter Visualization V2312. Corrected CVSSv3.1 vector of CVE-2023-38532. Added CVSSv4.0 vector to all CVEs
V1.3 (2024-08-13): Added fix version for Teamcenter Visualization V14.2 for CVE-2023-38527, CVE-2023-38529, CVE-2023-38531

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.