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

Publication Date: 2023-08-08
Last Update: 2023-11-14
Current Version: V1.1
CVSS v3.1 Base Score: 7.8

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 updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Parasolid V34.1: All versions < V34.1.258	Update to V34.1.258 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 < V35.0.254	Update to V35.0.254 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 < V35.1.171 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/en-US/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/en-US/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/en-US/product/258316782/ See further recommendations from section Workarounds and Mitigations

Teamcenter Visualization V14.1: All versions < V14.1.0.11	Update to V14.1.0.11 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Teamcenter Visualization V14.2: All versions < V14.2.0.6	Update to V14.2.0.6 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Teamcenter Visualization V14.3: All versions < V14.3.0.3	Update to V14.3.0.3 or later version https://support.sw.siemens.com/ 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 X_T 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 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-2023-38524

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
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
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
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
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
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
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
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
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	6.6
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C
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

TERMS OF USE