SSA-771940: X_T File Parsing Vulnerabilities in Teamcenter Visualization and JT2Go

Publication Date: 2024-06-11
Last Update: 2024-06-11
Current Version: V1.0
CVSS v3.1 Base Score: 7.8
CVSS v4.0 Base Score: 7.3

SUMMARY

Teamcenter Visualization and JT2Go is affected by out of bounds read, stack exhaustion and null pointer dereference 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 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 is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
JT2Go: All versions < V2312.0004 affected by all CVEs	Update to V2312.0004 or later version https://plm.sw.siemens.com/en-US/plm-components/jt/jt2go/ See further recommendations from section Workarounds and Mitigations
Teamcenter Visualization V14.2: All versions affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
Teamcenter Visualization V14.3: All versions < V14.3.0.9 affected by all CVEs	Update to V14.3.0.9 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Teamcenter Visualization V2312: All versions < V2312.0004 affected by all CVEs	Update to V2312.0004 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 XT files in Teamcenter Visualization and JT2Go

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

JT2Go is a 3D JT viewing tool to allow users to view JT, PDF, Solid Edge, PLM XML with available JT, VFZ, CGM, and TIF data.

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-2024-26275

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
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-2024-26276

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
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

Vulnerability CVE-2024-26277

The affected applications contain a null pointer dereference vulnerability while parsing specially crafted X_T 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
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 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 (2024-06-11): Publication Date

TERMS OF USE