SSA-700053: Multiple File Parsing Vulnerabilities in Teamcenter Visualization and JT2Go

Publication Date:	2022-12-13
Last Update:	2023-03-14
Current Version:	V1.1
CVSS v3.1 Base Score:	7.8

SUMMARY

Siemens Teamcenter Visualization and JT2Go are affected by multiple file parsing vulnerabilities that could be triggered when the application reads a malicious file in CGM or RAS format. If a user is tricked to open a malicious file with the affected products, this could lead the application to crash or potentially lead to arbitrary code execution.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
JT2Go: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
Teamcenter Visualization V13.2: All versions < V13.2.0.12	Update to V13.2.0.12 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Teamcenter Visualization V13.3: All versions < V13.3.0.9 only affected by CVE-2022-45484	Update to V13.3.0.9 or later version https://support.sw.siemens.com/ See recommendations from section Workarounds and Mitigations
Teamcenter Visualization V13.3: All versions < V13.3.0.8	Update to V13.3.0.8 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Teamcenter Visualization V14.0: All versions < V14.0.0.5 only affected by CVE-2022-45484	Update to V14.0.0.5 or later version https://support.sw.siemens.com/ See recommendations from section Workarounds and Mitigations
Teamcenter Visualization V14.0: All versions < V14.0.0.4	Update to V14.0.0.4 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Teamcenter Visualization V14.1: All versions < V14.1.0.6	Update to V14.1.0.6 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 CGM or RAS files in JT2Go and 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

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 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-2022-41278

The CGM_NIST_Loader.dll contains a null pointer dereference vulnerability while parsing specially crafted CGM 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
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2022-41279

The CGM_NIST_Loader.dll contains a null pointer dereference vulnerability while parsing specially crafted CGM 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
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2022-41280

The CGM_NIST_Loader.dll contains a null pointer dereference vulnerability while parsing specially crafted CGM 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
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2022-41281

The CGM_NIST_Loader.dll contains an out of bounds read vulnerability when parsing a CGM file. An attacker can leverage this vulnerability 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-2022-41282

The CGM_NIST_Loader.dll contains an out of bounds read vulnerability when parsing a CGM file. An attacker can leverage this vulnerability 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-2022-41283

The CGM_NIST_Loader.dll contains an out of bounds write vulnerability when parsing a CGM file. An attacker can leverage this vulnerability 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-2022-41284

The CGM_NIST_Loader.dll contains an out of bounds read vulnerability when parsing a CGM file. An attacker can leverage this vulnerability 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-2022-41285

The CGM_NIST_Loader.dll contains a use-after-free vulnerability that could be triggered while parsing specially crafted CGM files. An attacker could leverage this vulnerability 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-416: Use After Free

Vulnerability CVE-2022-41286

The CGM_NIST_Loader.dll contains an out of bounds write vulnerability when parsing a CGM file. An attacker can leverage this vulnerability 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-2022-41287

The CGM_NIST_Loader.dll contains divide by zero vulnerability when parsing a CGM file. 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
CWE	CWE-369: Divide By Zero

Vulnerability CVE-2022-41288

The CGM_NIST_Loader.dll contains stack exhaustion vulnerability when parsing a CGM file. 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
CWE	CWE-770: Allocation of Resources Without Limits or Throttling

Vulnerability CVE-2022-45484

The CCITT_G4Decode.dll contains an out of bounds read vulnerability when parsing a RAS file. An attacker can leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-19056)

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-125: Out-of-bounds Read

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Trend Micro Zero Day Initiative for coordinated disclosure of CVE-2022-45484
- Jin Huang from ADLab of Venustech for reporting the vulnerabilities CVE-2022-41278 - CVE-2022-41288

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 (2022-12-13):	Publication Date
V1.1 (2023-03-14):	Added remediation for Teamcenter Visualization version lines V13.3 and V14.0 for CVE-2022-45484

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.