SSA-622830: Multiple File Parsing Vulnerabilities in JT2Go and Teamcenter Visualization before V13.1.0

Publication Date:	2021-01-12
Last Update:	2021-05-17
Current Version:	V1.2
CVSS v3.1 Base Score:	7.8

SUMMARY

Siemens has released version V13.1.0 for JT2Go and Teamcenter Visualization to fix multiple vulnerabilities that could be triggered when the products read files in different file formats (JT, XML, CG4, CGM, PDF, RGB, SGI, TGA, PAR, PCX). If a user is tricked to opening of a malicious file with the affected products, this could lead to application crash, or potentially arbitrary code execution or data extraction on the target host system.

Siemens recommends to update to the latest versions and to limit opening of untrusted files from unknown sources in the affected products. Please refer to SSA-663999 [0] and SSA-695540 [1] for further information regarding later version updates.

Note: Previous versions of this advisory also contained the vulnerabilities CVE-2020-26989, CVE-2020-26990, and CVE-2020-28383 (now addressed in [0]) and CVE-2020-26991 (now addressed in [1]).

[0] https://cert-portal.siemens.com/productcert/pdf/ssa-663999.pdf

[1] https://cert-portal.siemens.com/productcert/pdf/ssa-695540.pdf

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
JT2Go: All versions < V13.1.0	Update to V13.1.0 or later version https://www.plm.automation.siemens.com/global/en/products/plm-components/jt2go.html
Teamcenter Visualization: All versions < V13.1.0	Update to V13.1.0 or later version https://support.sw.siemens.com/ (login required)

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Avoid to open untrusted files from unknown sources in JT2Go and Teamcenter Visualization

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-2020-26980

Affected applications lack proper validation of user-supplied data when parsing JT files. A crafted JT file could trigger a type confusion condition. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11881)

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-843: Access of Resource Using Incompatible Type ('Type Confusion')

Vulnerability CVE-2020-26981

When opening a specially crafted xml file, the application could disclose arbitrary files to remote attackers. This is because of the passing of specially crafted content to the underlying XML parser without taking proper restrictions such as prohibiting an external dtd. (ZDI-CAN-11890)

CVSS v3.1 Base Score	5.6
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-611: Improper Restriction of XML External Entity Reference

Vulnerability CVE-2020-26982

Affected applications lack proper validation of user-supplied data when parsing CG4 and CGM files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11898)

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-2020-26983

Affected applications lack proper validation of user-supplied data when parsing PDF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11900)

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-2020-26984

Affected applications lack proper validation of user-supplied data when parsing of JT files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11972)

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-2020-26985

Affected applications lack proper validation of user-supplied data when parsing of RGB and SGI files. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11986, ZDI-CAN-11994)

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-122: Heap-based Buffer Overflow

Vulnerability CVE-2020-26986

Affected applications lack proper validation of user-supplied data when parsing of JT files. This could lead to a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12014)

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-122: Heap-based Buffer Overflow

Vulnerability CVE-2020-26987

Affected applications lack proper validation of user-supplied data when parsing of TGA files. This could lead to a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12016, ZDI-CAN-12017)

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-122: Heap-based Buffer Overflow

Vulnerability CVE-2020-26988

Affected applications lack proper validation of user-supplied data when parsing of PAR files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11891)

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-2020-26992

Affected applications lack proper validation of user-supplied data when parsing CGM files. This could lead to a stack based buffer overflow while trying to copy to a buffer during font string handling. 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-121: Stack-based Buffer Overflow

Vulnerability CVE-2020-26993

Affected applications lack proper validation of user-supplied data when parsing CGM files. This could lead to a stack based buffer overflow while trying to copy to a buffer in the font index handling function. 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-121: Stack-based Buffer Overflow

Vulnerability CVE-2020-26994

Affected applications lack proper validation of user-supplied data when parsing of PCX files. This could result in a heap-based buffer overflow. 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-122: Heap-based Buffer Overflow

Vulnerability CVE-2020-26995

Affected applications lack proper validation of user-supplied data when parsing of SGI and RGB files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11992)

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-2020-26996

Affected applications lack proper validation of user-supplied data when parsing of CG4 files. This could result in a memory access past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12027)

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

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Trend Micro Zero Day Initiative for coordinated disclosure of CVE-2020-26980 through CVE-2020-26991, CVE-2020-26995, CVE-2020-26996 and CVE-2020-28383
- Carsten Eiram from Risk Based Security for coordinated disclosure of CVE-2020-26992, CVE-2020-26993, CVE-2020-26980 and CVE-2020-26986
- Cybersecurity and Infrastructure Security Agency (CISA) for coordination efforts

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 (2021-01-12):	Publication Date
V1.1 (2021-02-09):	Included fix information for CVE-2020-26989, CVE-2020-26990 and CVE-2020-26991, and reference to new advisory SSA-663999
V1.2 (2021-05-17):	Moved vulnerabilities CVE-2020-26989, CVE-2020-26990, and CVE-2020-28383 to advisory SSA-663999; moved CVE-2020-26991 to SSA-695540

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.