SSA-595101: Multiple File Parsing Vulnerabilities in JT2Go and Teamcenter Visualization before V13.2.0.5

Publication Date: 2021-12-14
Last Update: 2021-12-14
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

SUMMARY

Siemens has released version V13.2.0.5 for JT2Go and Teamcenter Visualization to fix multiple vulnerabilities that could be triggered when the products read maliciously crafted files in different file formats (PDF, JT, TIFF, CGM and TIF). If a user is tricked to open a malicious file with any of the affected products, this could lead the application to crash or potentially lead to arbitrary code execution.

Siemens recommends to update to the latest versions and to limit opening of untrusted files from unknown sources in the affected products.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
JT2Go: All versions < V13.2.0.5	Update to V13.2.0.5 or later version https://www.plm.automation.siemens.com/global/en/products/plm-components/jt2go.html See further recommendations from section Workarounds and Mitigations
Teamcenter Visualization: All versions < V13.2.0.5	Update to V13.2.0.5 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:

- 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-2021-44001

The DL180pdfl.dll contains an out of bounds write past the end of an allocated structure while parsing specially crafted PDF files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14974)

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-2021-44002

The Jt1001.dll contains an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15058)

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-2021-44003

The Tiff_Loader.dll is vulnerable to use of uninitialized memory while parsing user supplied TIFF files. This could allow an attacker to cause a 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:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-457: Use of Uninitialized Variable

Vulnerability CVE-2021-44004

The Tiff_Loader.dll is vulnerable to an out of bounds read past the end of an allocated buffer when parsing TIFF files. An attacker could leverage this vulnerability to leak information 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:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-44005

The Tiff_Loader.dll contains an out of bounds write past the end of an allocated structure while parsing specially crafted TIFF 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-787: Out-of-bounds Write

Vulnerability CVE-2021-44006

The Tiff_Loader.dll contains an out of bounds write past the end of an allocated structure while parsing specially crafted TIFF 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-787: Out-of-bounds Write

Vulnerability CVE-2021-44007

The Tiff_Loader.dll contains an off-by-one error in the heap while parsing specially crafted TIFF files. This could allow an attacker to cause a 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-193: Off-by-one Error

Vulnerability CVE-2021-44008

The Tiff_Loader.dll is vulnerable to an out of bounds read past the end of an allocated buffer when parsing TIFF files. An attacker could leverage this vulnerability to leak information 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:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-44009

The Tiff_Loader.dll is vulnerable to an out of bounds read past the end of an allocated buffer when parsing TIFF files. An attacker could leverage this vulnerability to leak information 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:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-44010

The Tiff_Loader.dll is vulnerable to an out of bounds read past the end of an allocated buffer when parsing TIFF files. An attacker could leverage this vulnerability to leak information 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:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-44011

The Jt1001.dll is vulnerable to an out of bounds read past the end of an allocated buffer while parsing specially crafted JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-15101)

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-44012

The Jt1001.dll is vulnerable to an out of bounds read past the end of an allocated buffer when parsing specially crafted JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-15102)

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-44013

The DL180pdfl.dll contains an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15103)

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-2021-44014

The Jt1001.dll contains a use-after-free vulnerability that could be triggered while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-15057)

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-2021-44015

The VCRUNTIME140.dll is vulnerable to an out of bounds read past the end of an allocated buffer when parsing specially crafted CGM files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-15109)

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-44017

The Image.dll is vulnerable to an out of bounds read past the end of an allocated buffer when parsing specially crafted TIF files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-15111)

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/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-2021-44001, CVE-2021-44002, CVE-2021-44017 and CVE-2021-44011 through CVE-2021-44015
- Cybersecurity and Infrastructure Security Agency (CISA) for coordinated disclosure
- Jin Huang from ADLab of Venustech for reporting the vulnerabilities from CVE-2021-44003 through CVE-2021-44010

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 (2021-12-14): Publication Date

TERMS OF USE