

## SSA-278349: Multiple WRL File Parsing Vulnerabilities in Teamcenter Visualization and JT2Go

Publication Date: 2023-09-12  
Last Update: 2023-09-12  
Current Version: V1.0  
CVSS v3.1 Base Score: 7.8

### SUMMARY

Siemens JT2Go and Teamcenter Visualization are affected by file parsing vulnerabilities that could be triggered when the application reads files in WRL format. 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 has released updates for several affected products and recommends to update to the latest versions. Siemens recommends countermeasures for products where updates are not, or not yet available.

### AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
JT2Go: All versions < V14.3.0.1	Update to V14.3.0.1 or later version <a href="https://www.plm.automation.siemens.com/global/en/products/plm-components/jt2go.html">https://www.plm.automation.siemens.com/global/en/products/plm-components/jt2go.html</a>
Teamcenter Visualization V13.3: All versions < V13.3.0.12	Update to V13.3.0.12 or later version <a href="https://support.sw.siemens.com/">https://support.sw.siemens.com/</a>
Teamcenter Visualization V14.0: All versions	Currently no fix is planned
Teamcenter Visualization V14.1: All versions < V14.1.0.11	Update to V14.1.0.11 or later version <a href="https://support.sw.siemens.com/">https://support.sw.siemens.com/</a>
Teamcenter Visualization V14.2: All versions < V14.2.0.6	Update to V14.2.0.6 or later version <a href="https://support.sw.siemens.com/">https://support.sw.siemens.com/</a>
Teamcenter Visualization V14.3: All versions < V14.3.0.1	Update to V14.3.0.1 or later version <a href="https://support.sw.siemens.com/">https://support.sw.siemens.com/</a>

### WORKAROUNDS AND MITIGATIONS

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-2023-38070**

The affected application is vulnerable to stack-based buffer overflow while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20818)

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">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</a>
CWE	CWE-121: Stack-based Buffer Overflow

### **Vulnerability CVE-2023-38071**

The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20824)

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">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</a>
CWE	CWE-122: Heap-based Buffer Overflow

### **Vulnerability CVE-2023-38072**

The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20825)

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">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</a>
CWE	CWE-787: Out-of-bounds Write

### **Vulnerability CVE-2023-38073**

The affected application contains a type confusion vulnerability while parsing WRL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20826)

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 Con-  
fusion')

### **Vulnerability CVE-2023-38074**

The affected application contains a type confusion vulnerability while parsing WRL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20840)

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 Con-  
fusion')

### **Vulnerability CVE-2023-38075**

The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted WRL files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-20842)

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-2023-38076**

The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21041)

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

## **ACKNOWLEDGMENTS**

Siemens thanks the following party for its efforts:

- Trend Micro Zero Day Initiative for coordinated disclosure

## **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 (2023-09-12): Publication Date

## **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](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.