

## **SSA-663999: Multiple File Parsing Vulnerabilities in JT2Go and Teamcenter Visualization before V13.1.0.1**

Publication Date: 2021-02-09  
Last Update: 2021-02-09  
Current Version: V1.0  
CVSS v3.1 Base Score: 7.8

### **SUMMARY**

Siemens has released version V13.1.0.1 for JT2Go and Teamcenter Visualization to fix multiple vulnerabilities that could be triggered when the products read files in different file formats (PAR, BMP, TIFF, CGM, TGA, PCT, HPG, PLT, RAS, ASM, DGN, DXF, DWG). 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.

### **AFFECTED PRODUCTS AND SOLUTION**

<b>Affected Product and Versions</b>	<b>Remediation</b>
JT2Go: All versions < V13.1.0.1	Update to V13.1.0.1 <a href="https://support.sw.siemens.com/">https://support.sw.siemens.com/</a> (login required)
Teamcenter Visualization: All versions < V13.1.0.1	Update to V13.1.0.1 <a href="https://support.sw.siemens.com/">https://support.sw.siemens.com/</a> (login required)

### **WORKAROUNDS AND MITIGATIONS**

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

- Siemens recommends to limit the opening of untrusted files from unknown sources in the affected products
- Applying a Defense-in-Depth concept can help to reduce the probability that untrusted code is run on the system. Siemens recommends to apply the Defense-in-Depth concept: <https://www.siemens.com/industrialsecurity>

### **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-2020-26998

Affected applications lack proper validation of user-supplied data when parsing of PAR files. This could result in a memory access past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information. (ZDI-CAN-12040)

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-125: Out-of-bounds Read

### Vulnerability CVE-2020-26999

Affected applications lack proper validation of user-supplied data when parsing of PAR files. This could result in a memory access past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information. (ZDI-CAN-12042)

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-125: Out-of-bounds Read

### Vulnerability CVE-2020-27000

Affected applications lack proper validation of user-supplied data when parsing BMP files. This can result in a memory corruption condition. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12018)

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-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

#### Vulnerability CVE-2020-27001

Affected applications lack proper validation of user-supplied data when parsing of PAR files. This could result in a stack based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12041)

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-2020-27002

Affected applications lack proper validation of user-supplied data when parsing of PAR files. This could result in a memory access past the end of an allocated buffer. An attacker could leverage this vulnerability to access data in the context of the current process. (ZDI-CAN-12043)

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-2020-27003

Affected applications lack proper validation of user-supplied data when parsing TIFF files. This could lead to pointer dereferences of a value obtained from untrusted source. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12158)

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-822: Untrusted Pointer Dereference

#### Vulnerability CVE-2020-27004

Affected applications lack proper validation of user-supplied data when parsing of CGM files. This could result in a memory access past the end of an allocated buffer. An attacker could leverage this vulnerability to access data in the context of the current process. (ZDI-CAN-12163)

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-2020-27005

Affected applications lack proper validation of user-supplied data when parsing of TGA 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-12178)

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-2020-27006

Affected applications lack proper validation of user-supplied data when parsing of PCT files. This could result in a memory corruption condition. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12182)

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-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2020-27007

Affected applications lack proper validation of user-supplied data when parsing of HPG files. This could result in a memory access past the end of an allocated buffer. An attacker could leverage this vulnerability to access data in the context of the current process. (ZDI-CAN-12207)

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-125: Out-of-bounds Read

Vulnerability CVE-2020-27008

Affected applications lack proper validation of user-supplied data when parsing of PLT files. This could result in a memory access past the end of an allocated buffer. An attacker could leverage this vulnerability to access data in the context of the current process. (ZDI-CAN-12209)

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-125: Out-of-bounds Read

Vulnerability CVE-2020-28394

Affected applications lack proper validation of user-supplied data when parsing of RAS files. This could result in a memory access past the end of an allocated buffer. An attacker could leverage this vulnerability to access data in the context of the current process. (ZDI-CAN-12283)

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-125: Out-of-bounds Read

Vulnerability CVE-2020-26989

Affected applications lack proper validation of user-supplied data when parsing of PAR files. This could result in a stack based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11892)

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-2020-26990

Affected applications lack proper validation of user-supplied data when parsing ASM files. A crafted ASM 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-11897)

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

Vulnerability CVE-2020-26991

Affected applications lack proper validation of user-supplied data when parsing ASM files. This could lead to pointer dereferences of a value obtained from untrusted source. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11899)

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-822: Untrusted Pointer Dereference

Vulnerability CVE-2021-25173

An issue was discovered in Open Design Alliance Drawings SDK before 2021.12. A memory allocation with excessive size vulnerability exists when reading malformed DGN files, which could allow attackers to cause a crash, potentially enabling denial of service (crash, exit, or restart). (ZDI-CAN-12019)

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-789: Uncontrolled Memory Allocation

Vulnerability CVE-2021-25174

An issue was discovered in Open Design Alliance Drawings SDK before 2021.12. A memory corruption vulnerability exists when reading malformed DGN files. It could allow attackers to cause a crash, potentially enabling denial of service (Crash, Exit, or Restart). (ZDI-CAN-12026)

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-789: Uncontrolled Memory Allocation

Vulnerability CVE-2021-25175

An issue was discovered in Open Design Alliance Drawings SDK before 2021.11. A Type Conversion issue exists when rendering malformed .DXF and .DWG files. This could allow attackers to cause a crash, potentially enabling a denial of service attack (Crash, Exit, or Restart). (ZDI-CAN-11912, ZDI-CAN-11993, ZDI-CAN-11988)

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-822: Untrusted Pointer Dereference

### Vulnerability CVE-2021-25176

An issue was discovered in Open Design Alliance Drawings SDK before 2021.11. A NULL pointer dereference exists when rendering malformed .DXF and .DWG files. This could allow attackers to cause a crash, potentially enabling a denial of service attack (Crash, Exit, or Restart). (ZDI-CAN-11913, ZDI-CAN-11989)

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-822: Untrusted Pointer Dereference

### Vulnerability CVE-2021-25177

An issue was discovered in Open Design Alliance Drawings SDK before 2021.11. A Type Confusion issue exists when rendering malformed .DXF and .DWG files. (ZDI-CAN-11927)

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

### Vulnerability CVE-2021-25178

An issue was discovered in Open Design Alliance Drawings SDK before 2021.11. A stack-based buffer overflow vulnerability exists when the recover operation is run with malformed .DXF and .DWG files. (ZDI-CAN-11901, ZDI-CAN-12165, ZDI-CAN-12166)

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

## **ACKNOWLEDGMENTS**

Siemens thanks the following parties for their efforts:

- Trend Micro Zero Day Initiative for coordinated disclosure
- Open Design Alliance for coordination efforts
- Cybersecurity and Infrastructure Security Agency (CISA) for coordination efforts

## **ADDITIONAL INFORMATION**

For more details regarding the vulnerabilities in Open Design Alliance (ODA) Drawings SDK (CVE-2021-25173 through CVE-2021-25178) refer to:

- [ODA Security Advisories](#)

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 (2021-02-09): 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.