# SSA-429204 Open Design Alliance Drawings SDK Vulnerabilities in JT2Go and Teamcenter Visualization

Publication Date: 2022-07-12
Last Update: 2022-09-13
Current Version: V1.2
CVSS v3.1 Base Score: 7.8

## SUMMARY

JT2Go and Teamcenter Visualization are affected by multiple file parsing vulnerabilities in Drawings SDK from Open Design Alliance. If a user is tricked to open a malicious DWG 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 the affected products and recommends to update to the latest versions.

Note:

- This advisory covers security vulnerabilities recently disclosed by Open Design Alliance [0]

[0] https://www.opendesign.com/security-advisories

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| JT2Go:<br>All versions < V13.3.0.5 | Update to V13.3.0.5 or later version<br>https://www.plm.automation.siemens.com/global/en/products/plm-components/jt2go.html<br>See further recommendations from section Workarounds and Mitigations |
| Teamcenter Visualization V12.4:<br>All versions < V12.4.0.15 | Update to V12.4.0.15 or later version<br>https://support.sw.siemens.com/<br>See further recommendations from section Workarounds and Mitigations |
| Teamcenter Visualization V13.2:<br>All versions < V13.2.0.9 | Update to V13.2.0.9 or later version<br>https://support.sw.siemens.com/<br>See further recommendations from section Workarounds and Mitigations |
| Teamcenter Visualization V13.3:<br>All versions < V13.3.0.5 | Update to V13.3.0.5 or later version<br>https://support.sw.siemens.com/<br>See further recommendations from section Workarounds and Mitigations |
| Teamcenter Visualization V14.0:<br>All versions < V14.0.0.2 | Update to V14.0.0.2 or later version<br>https://support.sw.siemens.com/<br>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

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-2022-28807

Open Design Alliance Drawings SDK (all versions prior to 2023.2) is vulnerable to an out-of-bounds read when rendering DWG files after they are opened in the recovery mode. 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-125: Out-of-bounds Read |

### Vulnerability CVE-2022-28808

Open Design Alliance Drawings SDK (all versions prior to 2023.3) is vulnerable to an out-of-bounds read when reading DWG files in a recovery mode. 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-125: Out-of-bounds Read |

### Vulnerability CVE-2022-28809

Open Design Alliance Drawings SDK (all versions prior to 2023.3) is vulnerable to an out-of-bounds read when reading a DWG file with invalid vertex number in a recovery mode. 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-125: Out-of-bounds Read |

## ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Open Design Alliance for coordination efforts
- Yonghui Han from FortiGuard Labs for coordinated disclosure

## ADDITIONAL INFORMATION

For more details regarding the vulnerabilities in Open Design Alliance (ODA) Drawings SDK refer to the ODA Security Advisories at https://www.opendesign.com/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 (2022-07-12): | Publication Date |
| V1.1 (2022-08-09): | Added fix for Teamcenter Visualization version lines V13.2 and V14.0 |
| V1.2 (2022-09-13): | Added fix for Teamcenter Visualization version line V12.4 |

## 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.