SSA-365397: Multiple File Parsing Vulnerabilities in JT2Go and Teamcenter Visualization before V13.2.0.1

Publication Date: 2021-08-10
Last Update: 2021-08-10
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

SUMMARY

Siemens has released version V13.2.0.1 for JT2Go and Teamcenter Visualization to fix multiple vulnerabilities that could be triggered when the products read files in different file formats (CGM, DGN, DXF, and DWG). If a user is tricked to open a malicious file with the affected products, this could lead the application to crash or potentially 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.

Note:

- This advisory also 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: All versions < V13.2.0.1	Update to V13.2.0.1 or later version https://www.plm.automation.siemens.com/global/en/products/plm-components/jt2go.html
Teamcenter Visualization: All versions < V13.2.0.1	Update to V13.2.0.1 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-2021-32936

An out-of-bounds write issue exists in the DXF file-recovering procedure in the Open Design Alliance Drawings SDK (All versions prior to 2022.4) resulting from the lack of proper validation of user-supplied data. This can result in a write past the end of an allocated buffer and allow attackers to cause a denial-of-service condition or 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-2021-32938

Open Design Alliance Drawings SDK (All versions prior to 2022.4) are vulnerable to an out-of-bounds read due to parsing of DWG files resulting from the lack of proper validation of user-supplied data. This can result in a read past the end of an allocated buffer and allows attackers to cause a denial-of service condition or read sensitive information from memory.

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-32940

An out-of-bounds read issue exists in the DWG file-recovering procedure in the Open Design Alliance Drawings SDK (All versions prior to 2022.4) resulting from the lack of proper validation of user-supplied data. This can result in a read past the end of an allocated buffer and allow attackers to cause a denial-of-service condition or read sensitive information from memory locations.

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-32944

A use-after-free issue exists in the DGN file-reading procedure in the Open Design Alliance Drawings SDK (All versions prior to 2022.4) resulting from the lack of proper validation of user-supplied data. This can result in a memory corruption or arbitrary code execution, allowing attackers to cause a denial-of-service condition or 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-416: Use After Free

Vulnerability CVE-2021-32948

An out-of-bounds write issue exists in the DWG file-reading procedure in the Open Design Alliance Drawings SDK (All versions prior to 2022.4) resulting from the lack of proper validation of user-supplied data. This can result in a write past the end of an allocated buffer and allow attackers to cause a denial-of-service condition or 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-2021-32950

An out-of-bounds read issue exists within the parsing of DXF files in the Open Design Alliance Drawings SDK (All versions prior to 2022.4) resulting from the lack of proper validation of user-supplied data. This can result in a read past the end of an allocated buffer and allows attackers to cause a denial-of-service condition or read sensitive information from memory locations.

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-33717

When parsing specially crafted CGM Files, a NULL pointer deference condition could cause the application to crash. The application must be restarted to restore the service. An attacker could leverage this vulnerability to cause a Denial-of-Service condition in the application.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Trend Micro Zero Day Initiative for coordinated disclosure
- Open Design Alliance for coordination efforts
- Kai Wang from Codesafe Team of Legendsec at Qi'anxin Group for coordinated disclosure of CVE-2021-33717

ADDITIONAL INFORMATION

For more details regarding the vulnerabilities in Open Design Alliance (ODA) Drawings SDK (CVE-2021-32936, CVE-2021-32938, CVE-2021-32940, CVE-2021-32944, CVE-2021-32948 and CVE-2021-32950) 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 (2021-08-10): Publication Date

TERMS OF USE