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

Publication Date: 2021-02-09
Last Update: 2021-05-17
Current Version: V1.1
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 (BMP, TIFF, CGM, TGA, PCT, HPG, PLT, RAS, PAR, ASM, 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.

Notes:

- Previous versions of this advisory incorrectly listed the following vulnerabilities as being fixed in V13.1.0.1: CVE-2020-26991, CVE-2020-26998, CVE-2020-26999, CVE-2020-27001 and CVE-2020-27002. Those were fixed in V13.1.0.2 and are therefore addressed in advisory SSA-695540 [0]
- The vulnerability CVE-2020-28383 was incorrectly listed in SSA-622830 [1] as being fixed in V13.1.0.0. This was fixed in V13.1.0.1 and therefore added here
- The Open Design Alliance [2] recently disclosed an additional vulnerability (CVE-2021-31784) which is also covered in this advisory

[0] https://cert-portal.siemens.com/productcert/pdf/ssa-622830.pdf

[1] https://cert-portal.siemens.com/productcert/pdf/ssa-695540.pdf

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
JT2Go: All versions < V13.1.0.1	Update to V13.1.0.1 or later version https://www.plm.automation.siemens.com/global/en/products/plm-components/jt2go.html
Teamcenter Visualization: All versions < V13.1.0.1	Update to V13.1.0.1 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-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	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-2020-26990

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	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 Confusion')

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

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	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-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	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-2020-27008

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	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-2020-28383

Affected applications lack proper validation of user-supplied data when parsing PAR files. This can result in an out of bounds write past the memory location that is a read only image address. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11885)

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-2020-28394

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	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-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	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-789: Memory Allocation with Excessive Size Value

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	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-789: Memory Allocation with Excessive Size Value

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	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-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	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-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	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 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	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-2021-31784

An out-of-bounds write vulnerability exists in the file-reading procedure in Open Design Alliance Drawings SDK before 2021.6.

This could allow an attacker to cause a crash, potentially enabling a denial of service attack (Crash, Exit, or Restart) or possible code execution. (ZDI-CAN-11915)

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

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 and CVE-2021-31784) 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
V1.1 (2021-05-17):	Removed the vulnerabilities CVE-2020-26991, CVE-2020-26998, CVE-2020-26999, CVE-2020-27001, CVE-2020-27002, and added CVE-2020-28383, CVE-2021-31784 for the reasons described in the Summary

TERMS OF USE