SSA-301589: Multiple File Parsing Vulnerabilities in Solid Edge, JT2Go and Teamcenter Visualization

Publication Date: 2022-02-08
Last Update: 2022-06-14
Current Version: V1.3
CVSS v3.1 Base Score: 7.8

SUMMARY

Siemens has released updates for JT2Go, Solid Edge and Teamcenter Visualization to fix multiple file parsing vulnerabilities. If a user is tricked to open a malicious file (crafted as PDF, DXF or PAR) 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 some of the affected products and recommends to update to the latest versions. Siemens is preparing further updates and recommends specific countermeasures for products where updates are not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
JT2Go: All versions < V13.2.0.7	Update to V13.2.0.7 or later version https://www.plm.automation.siemens.com/global/en/products/plm-components/jt2go.html See further recommendations from section Workarounds and Mitigations
Solid Edge SE2021: All versions < SE2021MP9 only affected by CVE-2021-44000, CVE-2021-44016, CVE-2021-44018	Update to SE2021MP9 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Solid Edge SE2022: All versions < SE2022MP1 only affected by CVE-2021-44000, CVE-2021-44016, CVE-2021-44018	Update to SE2022MP1 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Teamcenter Visualization V12.4: All versions < V12.4.0.13 only affected by CVE-2021-38405, CVE-2021-43336	Update to V12.4.0.13 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Teamcenter Visualization V13.1: All versions < V13.1.0.8 only affected by CVE-2021-38405	Update to V13.1.0.8 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Teamcenter Visualization V13.1: All versions < V13.1.0.9 only affected by CVE-2021-43336, CVE-2021-44000, CVE-2021-44016, CVE-2021-44018	Update to V13.1.0.9 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations

Teamcenter Visualization V13.2: All versions < V13.2.0.7	Update to V13.2.0.7 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Teamcenter Visualization V13.3: All versions < V13.3.0.1	Update to V13.3.0.1 or later version https://support.sw.siemens.com/ 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 affected products

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.

Solid Edge is a portfolio of software tools that addresses various product development processes: 3D design, simulation, manufacturing and design management.

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-2021-38405

The Datalogics APDFL library used in affected products is vulnerable to memory corruption condition while parsing specially crafted PDF files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-15106, ZDI-CAN-15108, ZDI-CAN-15113)

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:T/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2021-43336

Open Design Alliance Drawings SDK before 2022.11 used in affected products contains an out of bounds write vulnerability when parsing a DXF file. An attacker can leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-15107)

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-2021-44000

The plmxmlAdapterSE70.dll contains an out of bounds write past the fixed-length heap-based buffer while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15053)

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

Vulnerability CVE-2021-44016

The plmxmlAdapterSE70.dll library is vulnerable to memory corruption condition while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-15110)

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-2021-44018

The plmxmlAdapterSE70.dll library is vulnerable to memory corruption condition while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-15112)

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:

- Trend Micro Zero Day Initiative for coordinated disclosure

ADDITIONAL INFORMATION

This advisory also covers security vulnerabilities disclosed by Open Design Alliance (CVE-2021-43336) [0] and Datalogics (CVE-2021-38405) [1].

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

[1] Datalogics Release Notes SF#44621: https://dev.datalogics.com/adobe-pdf-library/release-notes-adobe-pdf-library-v-18/

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 (2022-02-08):	Publication Date
V1.1 (2022-03-08):	Added remediation for Teamcenter Visualization version lines V12.4 and V13.3
V1.2 (2022-04-12):	Added remediation for Teamcenter Visualization version line V13.2 and JT2Go
V1.3 (2022-06-14):	Added fix for CVE-2021-43336, CVE-2021-44000, CVE-2021-44016 and CVE-2021-44018 in Teamcenter Visualization version line V13.1

TERMS OF USE