SSA-695540: ASM and PAR File Parsing Vulnerabilities in JT2Go and Teamcenter Visualization before V13.1.0.2

Publication Date: 2021-05-17
Last Update: 2021-05-17
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

SUMMARY

Siemens has released version V13.1.0.2 for JT2Go and Teamcenter Visualization to fix multiple vulnerabilities that could be triggered when the products read files in ASM and PAR file formats. 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

Affected Product and Versions	Remediation
JT2Go: All versions < V13.1.0.2	Update to V13.1.0.2 or later version https://www.plm.automation.siemens.com/global/en/products/plm-components/jt2go.html
Teamcenter Visualization: All versions < V13.1.0.2	Update to V13.1.0.2 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-2020-26991

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	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-2020-26998

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	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-2020-26999

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	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-2020-27001

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

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Trend Micro Zero Day Initiative for coordinated disclosure
- Carsten Eiram from Risk Based Security for coordinated disclosure of CVE-2020-26991
- Cybersecurity and Infrastructure Security Agency (CISA) for coordination efforts

ADDITIONAL INFORMATION

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 (2021-05-17): Publication Date

TERMS OF USE