

## SSA-611756: JT File Parsing Vulnerability in JTTK and Simcenter Femap

Publication Date: 2022-10-11  
Last Update: 2022-10-11  
Current Version: V1.0  
CVSS v3.1 Base Score: 7.8

### SUMMARY

JT Open Toolkit (JTTK) and Simcenter Femap are affected by an uninitialized pointer reference vulnerability that could be triggered while parsing JT files. If a user is tricked to open a malicious JT file with any of the affected products, this could cause 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.

### AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
JTTK: All versions < V11.1.1.0	Update to V11.1.1.0 or later version <a href="https://support.sw.siemens.com/">https://support.sw.siemens.com/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
Simcenter Femap V2022.1: All versions < V2022.1.3	Update to V2022.1.3 or later version <a href="https://support.sw.siemens.com/">https://support.sw.siemens.com/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
Simcenter Femap V2022.2: All versions < V2022.2.2	Update to V2022.2.2 or later version <a href="https://support.sw.siemens.com/">https://support.sw.siemens.com/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

### WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Do not open untrusted files using JTTK or Simcenter Femap

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**

JT Open Toolkit (also known as JTTK) is an application programming interface (API) for developers of JT-enabled software. The JT Open Toolkit is a read/write toolkit that enables consistent access to JT file content.

Simcenter Femap is an advanced simulation application for creating, editing, and inspecting finite element models of complex products or systems.

## **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-2022-41851**

The JTTK library is vulnerable to an uninitialized pointer reference vulnerability while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-16973)

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-824: Access of Uninitialized Pointer

## **ACKNOWLEDGMENTS**

Siemens thanks the following party for its efforts:

- Trend Micro Zero Day Initiative for coordinated disclosure

## **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 (2022-10-11): Publication Date

## **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](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.