

## **SSA-352143: Multiple File Parsing Vulnerabilities in JTTK before V11.0.3.0 and JT Utilities before V13.0.3.0**

Publication Date: 2021-12-14  
Last Update: 2021-12-14  
Current Version: V1.0  
CVSS v3.1 Base Score: 7.8

### **SUMMARY**

JT Open Toolkit (JTTK) before V11.0.3.0 contains multiple vulnerabilities that could be triggered when the affected product reads a maliciously crafted JT file. These vulnerabilities also affects JT Utilities before V13.0.3.0. If a user is tricked to open a malicious file with any of the affected products, this could lead the application to crash or potentially lead to 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.

### **AFFECTED PRODUCTS AND SOLUTION**

<b>Affected Product and Versions</b>	<b>Remediation</b>
JT Utilities: All versions < V13.0.3.0	Update to V13.0.3.0 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>
JTTK: All versions < V11.0.3.0	Update to V11.0.3.0 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>

### **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 using JTTK
- Avoid to open untrusted files from unknown sources using JT Utilities

### **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 is an openly published data format developed by Siemens Digital Industries Software, widely used for communication, visualization, digital mockup and a variety of other purposes. JT has been accepted by

ISO as International Standard 14306:2017. The JT Utilities provide a series of command line utilities that can be used to support application development and JT reuse.

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.

## **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-2021-44446

JTTK library in affected products contains an out of bounds write past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14828, ZDI-CAN-14898)

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">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</a>
CWE	CWE-787: Out-of-bounds Write

### Vulnerability CVE-2021-44447

JTTK library in affected products contains a use-after-free vulnerability that could be triggered while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-14911)

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">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</a>
CWE	CWE-416: Use After Free

### Vulnerability CVE-2021-44448

JTTK library in affected products is vulnerable to an out of bounds read past the end of an allocated buffer when parsing JT files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-14843, ZDI-CAN-15051)

CVSS v3.1 Base Score	3.3
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C</a>
CWE	CWE-125: Out-of-bounds Read

## **ACKNOWLEDGMENTS**

Siemens thanks the following parties for their efforts:

- Bentley Systems Incorporated 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 (2021-12-14): 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.