SSA-209268: Multiple JT File Parsing Vulnerabilities in JT Utilities before V13.0.2.0

Publication Date:	2021-07-13
Last Update:	2021-07-13
Current Version:	V1.0
CVSS v3.1 Base Score:	5.5

SUMMARY

Siemens has released version V13.0.2.0 for JT Utilities to fix multiple vulnerabilities that could be triggered when reading JT files.

Siemens recommends to update to the latest version, which contains solutions to all the vulnerabilities listed in this advisory. Standing recommendation is to avoid opening of untrusted files from unknown sources in the affected product, as this generally mitigates the risk of exploitation of this class of vulnerabilities for any product release.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
JT Utilities: All versions < V13.0.2.0	Update to V13.0.2.0 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 opening untrusted files from unknown sources in 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.

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-2021-33713

When parsing specially crafted JT files, a hash function is called with an incorrect argument leading the application to crash. An attacker could leverage this vulnerability to cause a Denial-of-Service condition in the application.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-688: Function Call With Incorrect Variable or Reference as Argument

Vulnerability CVE-2021-33714

When parsing specially crafted JT files, a missing check for the validity of an iterator leads to NULL pointer deference condition, causing the application to crash. An attacker could leverage this vulnerability to cause a Denial-of-Service condition in the application.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2021-33715

When parsing specially crafted JT files, a race condition could cause an object to be released before being operated on, leading to NULL pointer deference condition and causing the application to crash. An attacker could leverage this vulnerability to cause a Denial-of-Service condition in the application.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- LeeJet from ICICS CO.,LTD for reporting the vulnerabilities

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 (2021-07-13): 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, 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.