

SSA-836777: JT File Parsing Vulnerabilities in JT Open, JT Utilities and Parasolid

Publication Date: 2023-02-14
 Last Update: 2023-02-14
 Current Version: V1.0
 CVSS v3.1 Base Score: 7.8

SUMMARY

JT Open Toolkit, JT Utilities and Parasolid are affected by memory corruption vulnerabilities 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
JT Open: All versions < V11.2.3.0 only affected by CVE-2022-47936, CVE-2022-47977	Update to V11.2.3.0 or later version https://support.sw.siemens.com/ See recommendations from section Workarounds and Mitigations
JT Utilities: All versions < V13.2.3.0 only affected by CVE-2022-47936, CVE-2022-47977	Update to V13.2.3.0 or later version https://support.sw.siemens.com/ See recommendations from section Workarounds and Mitigations
Parasolid V34.0: All versions < V34.0.252 only affected by CVE-2022-47936	Update to V34.0.252 or later version https://support.sw.siemens.com/ See recommendations from section Workarounds and Mitigations
Parasolid V34.0: All versions < V34.0.254 only affected by CVE-2023-25140	Update to V34.0.254 or later version https://support.sw.siemens.com/ See recommendations from section Workarounds and Mitigations
Parasolid V34.1: All versions < V34.1.242 only affected by CVE-2022-47936, CVE-2023-25140	Update to V34.1.242 or later version https://support.sw.siemens.com/ See recommendations from section Workarounds and Mitigations
Parasolid V35.0: All versions < V35.0.170 only affected by CVE-2022-47936, CVE-2023-25140	Update to V35.0.170 or later version https://support.sw.siemens.com/ See recommendations from section Workarounds and Mitigations
Parasolid V35.1: All versions < V35.1.150 only affected by CVE-2022-47936, CVE-2023-25140	Update to V35.1.150 or later version https://support.sw.siemens.com/ See 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:

- Do not open untrusted files using Parasolid, JT Open Toolkit or JT Utilities

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 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.

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.

Parasolid is a 3D geometric modeling tool that supports various techniques, including solid modeling, direct editing, and free-form surface/sheet modeling.

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-2022-47936

The affected application contains a stack overflow vulnerability while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process.

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-2022-47977

The affected application contains a memory corruption vulnerability while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process.

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-2023-25140

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.

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 party for its efforts:

- Michael Heinzl for reporting the vulnerability

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 (2023-02-14): 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, 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.