SSA-764801: File Parsing Vulnerabilities in Tecnomatix Plant Simulation

Publication Date: 2023-07-11
Last Update: 2023-09-12
Current Version: V1.2
CVSS v3.1 Base Score: 7.8

SUMMARY

Siemens Tecnomatix Plant Simulation contains multiple vulnerabilities that could be triggered when the application reads PAR, SPP, STP and PRT files. If a user is tricked to open a malicious file using the affected application, this could lead to a crash, and potentially also to arbitrary code execution on the target host system.

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
Tecnomatix Plant Simulation V2201: All versions < V2201.0008	Update to V2201.0008 or later version https://support.sw.siemens.com/ See recommendations from section Workarounds and Mitigations
Tecnomatix Plant Simulation V2302: All versions < V2302.0002	Update to V2302.0002 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 PAR, SPP, STP or PRT files from unknown sources

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

Tecnomatix Plant Simulation allows you to model, simulate, explore and optimize logistics systems and their processes. These models enable analysis of material flow, resource utilization and logistics for all levels of manufacturing planning from global production facilities to local plants and specific lines, well in advance of production execution.

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-2023-37246

The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted PRT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21109)

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-122: Heap-based Buffer Overflow

Vulnerability CVE-2023-37247

The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21138)

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-122: Heap-based Buffer Overflow

Vulnerability CVE-2023-37248

The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted PAR file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21155)

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-787: Out-of-bounds Write

Vulnerability CVE-2023-37374

The affected application is vulnerable to stack-based buffer overflow while parsing specially crafted STP files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21054)

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-2023-37375

The affected application is vulnerable to stack-based buffer overflow while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21060)

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-2023-37376

The affected application contains a type confusion vulnerability while parsing STP files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21051)

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-843: Access of Resource Using Incompatible Type (’Type Confusion’)

Vulnerability CVE-2023-38679

The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21106)

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-787: Out-of-bounds Write

Vulnerability CVE-2023-38680

The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21132)

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-787: Out-of-bounds Write

Vulnerability CVE-2023-38681

The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted IGS file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21270)

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-787: Out-of-bounds Write

Vulnerability CVE-2023-41846

The affected application is vulnerable to memory corruption while parsing specially crafted SPP 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

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Michael Heinzl for coordinated disclosure of CVE-2023-41846
- 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 (2023-07-11):	Publication Date
V1.1 (2023-08-08):	Added additional vulnerabilities CVE-2023-38679, CVE-2023-38680, CVE-2023-38681 that are fixed in the same product versions (V2201.0008, V2302.0002)
V1.2 (2023-09-12):	Added CVE-2023-41846 fixed in the same product versions (V2201.0008, V2302.0002)

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.