SSA-900277: MODEL File Parsing Vulnerability in Tecnomatix Plant Simulation before V2302.0012 and V2024.0001

Publication Date:	2024-06-11
Last Update:	2024-06-11
Current Version:	V1.0
CVSS v3.1 Base Score:	7.8
CVSS v4.0 Base Score:	7.3

SUMMARY

Tecnomatix Plant Simulation contains a type confusion vulnerability that could be triggered when the application reads MODEL 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 new versions for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Tecnomatix Plant Simulation V2302: All versions < V2302.0012 affected by CVE-2024-35303	Update to V2302.0012 or later version https://support.sw.siemens.com/en-US/product/297028302/ See further recommendations from section Workarounds and Mitigations
Tecnomatix Plant Simulation V2404: All versions < V2404.0001 affected by CVE-2024-35303	Update to V2404.0001 or later version https://support.sw.siemens.com/en-US/product/297028302/ See further 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 MODEL 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 DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2024-35303

The affected applications contain a type confusion vulnerability while parsing specially crafted MODEL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-22958)

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
CVSS v4.0 Base Score	7.3
CVSS Vector	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-704: Incorrect Type Conversion or Cast

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 (2024-06-11):	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, 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.