SSA-824503: Multiple WRL File Parsing Vulnerabilities in Tecnomatix Plant Simulation Before V2302.0018 and V2404.0007

Publication Date: 2024-11-18
Last Update: 2024-11-18
Current Version: V1.0
CVSS v3.1 Base Score: 7.8
CVSS v4.0 Base Score: 7.3

SUMMARY

Siemens Tecnomatix Plant Simulation contains multiple file parsing vulnerabilities that could be triggered when the application reads files in WRL format. 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 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 < V2302.0018 affected by all CVEs	Update to V2302.0018 or later version https://support.sw.siemens.com/product/297028302/ See further recommendations from section Workarounds and Mitigations
Tecnomatix Plant Simulation V2404: All versions < V2404.0007 affected by all CVEs	Update to V2404.0007 or later version https://support.sw.siemens.com/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:

- CVE-2024-52565, CVE-2024-52566, CVE-2024-52567, CVE-2024-52568, CVE-2024-52569, CVE-2024-52570, CVE-2024-52571, CVE-2024-52572, CVE-2024-52573, CVE-2024-52574: Do not open untrusted WRL files in affected applications

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-2024-52565

The affected applications contain an out of bounds write vulnerability when parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-24231)

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-787: Out-of-bounds Write

Vulnerability CVE-2024-52566

The affected applications contain an out of bounds write vulnerability when parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-24233)

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-787: Out-of-bounds Write

Vulnerability CVE-2024-52567

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-24237)

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-125: Out-of-bounds Read

Vulnerability CVE-2024-52568

The affected applications contain a use-after-free vulnerability that could be triggered while parsing specially crafted WRL files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-24244)

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-416: Use After Free

Vulnerability CVE-2024-52569

The affected applications contain an out of bounds write vulnerability when parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-24260)

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-787: Out-of-bounds Write

Vulnerability CVE-2024-52570

The affected applications contain an out of bounds write vulnerability when parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-24365)

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-787: Out-of-bounds Write

Vulnerability CVE-2024-52571

The affected applications contain an out of bounds write vulnerability when parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-24485)

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-787: Out-of-bounds Write

Vulnerability CVE-2024-52572

The affected applications contain a stack based overflow vulnerability while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-24486)

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-121: Stack-based Buffer Overflow

Vulnerability CVE-2024-52573

The affected applications contain an out of bounds write vulnerability when parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-24521)

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-787: Out-of-bounds Write

Vulnerability CVE-2024-52574

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-24543)

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-125: Out-of-bounds Read

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 (2024-11-18): Publication Date

TERMS OF USE

The use of Siemens Security Advisories is subject to the terms and conditions listed on: https://www.siemens.com/productcert/terms-of-use.