SSA-017796: Multiple File Parsing Vulnerabilities in Tecnomatix Plant Simulation

Publication Date: 2024-02-13
Last Update: 2024-02-13
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, PSOBJ or SPP file formats. 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 several affected products and recommends to update to the latest versions. Siemens recommends specific countermeasures for products where fixes are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Tecnomatix Plant Simulation V2201: All versions < V2201.0012 affected by CVE-2024-23795, CVE-2024-23796, CVE-2024-23797, CVE-2024-23798, CVE-2024-23802, CVE-2024-23804	Update to V2201.0012 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Tecnomatix Plant Simulation V2201: All versions affected by CVE-2024-23799, CVE-2024-23800, CVE-2024-23801, CVE-2024-23803	Currently no fix is planned See recommendations from section Workarounds and Mitigations
Tecnomatix Plant Simulation V2302: All versions < V2302.0006 affected by CVE-2024-23795, CVE-2024-23796, CVE-2024-23797, CVE-2024-23798, CVE-2024-23802, CVE-2024-23804	Update to V2302.0006 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Tecnomatix Plant Simulation V2302: All versions < V2302.0007 affected by CVE-2024-23799, CVE-2024-23800, CVE-2024-23801, CVE-2024-23803	Update to V2302.0007 or later version https://support.sw.siemens.com/ 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 WRL, PSOBJ, or SPP files from using Tecnomatix Plant Simulation

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-2024-23795

The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted WRL file. 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
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-2024-23796

The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted WRL 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
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-122: Heap-based Buffer Overflow

Vulnerability CVE-2024-23797

The affected applications contain a stack overflow vulnerability while parsing specially crafted WRL 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
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-2024-23798

The affected applications contain a stack overflow vulnerability while parsing specially crafted WRL 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
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-2024-23799

The affected applications contain a null pointer dereference vulnerability while parsing specially crafted SPP files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CVSS v4.0 Base Score	4.8
CVSS Vector	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2024-23800

The affected applications contain a null pointer dereference vulnerability while parsing specially crafted SPP files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CVSS v4.0 Base Score	4.8
CVSS Vector	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2024-23801

The affected applications contain a null pointer dereference vulnerability while parsing specially crafted SPP files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CVSS v4.0 Base Score	4.8
CVSS Vector	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2024-23802

The affected applications contain an out of bounds read past the end of an allocated structure 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
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-2024-23803

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.

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
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-2024-23804

The affected applications contain a stack overflow vulnerability while parsing specially crafted PSOBJ 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
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

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Michael Heinzl for coordinated disclosure of CVE-2024-23804
- Trend Micro Zero Day Initiative for coordinated disclosure of CVE-2024-23795, CVE-2024-23796, CVE-2024-23797 and CVE-2024-23798
- Nafiez from Logix Advisor for reporting the vulnerabilities CVE-2024-23799, CVE-2024-23800, CVE-2024-23801, CVE-2024-23802 and CVE-2024-23803

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 (2024-02-13): Publication Date

TERMS OF USE