SSA-478780: Multiple WRL File Parsing Vulnerabilities in Tecnomatix Plant Simulation

Publication Date: 2023-11-14
Last Update: 2023-11-14
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

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 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 < V2201.0010	Update to V2201.0010 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Tecnomatix Plant Simulation V2302: All versions < V2302.0004	Update to V2302.0004 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 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 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-2023-38070

The affected application is vulnerable to stack-based buffer overflow while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20818)

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-2023-38071

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. (ZDI-CAN-20824)

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-2023-38072

The affected application contains an out of bounds write 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-20825)

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-2023-38073

The affected application contains a type confusion vulnerability while parsing WRL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20826)

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-2023-38074

The affected application contains a type confusion vulnerability while parsing WRL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20840)

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-2023-38075

The affected application contains 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-20842)

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-416: Use After Free

Vulnerability CVE-2023-38076

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. (ZDI-CAN-21041)

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

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 (2023-11-14): Publication Date

TERMS OF USE