



# CVE-2023-24988

Published on: Not Yet Published

Last Modified on: 02/22/2023 08:25:00 PM UTC

## CVE-2023-24988

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Tecnomatix Plant Simulation](#) from [Siemens](#) contain the following vulnerability:

A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). 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-19810)

CVE-2023-24988 has been assigned by [S](#) productcert@siemens.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [S](#) **Siemens - Tecnomatix Plant Simulation** version = **All versions < V2201.0006**

CVSS3 Score: **7.8 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>LOCAL</b>     | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

## CVE References

| Description | Tags                                                                       | Link                                                                        |
|-------------|----------------------------------------------------------------------------|-----------------------------------------------------------------------------|
|             | <a href="#">cert-portal.siemens.com</a><br><a href="#">application/pdf</a> | <a href="#">MISC cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf</a> |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](#).

There are currently no QIDs associated with this CVE

| Known Affected Configurations (CPE V2.3)                                                       |                                                                                                                                                                                                                                                                                      |                             |                          |        |         |                     |
|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|--------------------------|--------|---------|---------------------|
| Type                                                                                           | Vendor                                                                                                                                                                                                                                                                               | Product                     | Version                  | Update | Edition | Language            |
| Application                                                                                    | Siemens                                                                                                                                                                                                                                                                              | Tecnomatix Plant Simulation | All                      | All    | All     | All                 |
| cpe:2.3:a:siemens:tecnomatix_plant_simulation:*****:                                           |                                                                                                                                                                                                                                                                                      |                             |                          |        |         |                     |
| No vendor comments have been submitted for this CVE                                            |                                                                                                                                                                                                                                                                                      |                             |                          |        |         |                     |
| Social Mentions                                                                                |                                                                                                                                                                                                                                                                                      |                             |                          |        |         |                     |
| Source                                                                                         | Title                                                                                                                                                                                                                                                                                |                             |                          |        |         | Posted (UTC)        |
|  @CVereport    | CVE-2023-24988 : A vulnerability has been identified in Tecnomatix Plant Simulation All versions < V2201.0006 . Th... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>                                                                              |                             |                          |        |         | 2023-02-14 11:20:13 |
|  @RedPacketSec | Siemens Tecnomatix Plant Simulation code execution   CVE-2023-24988 - <a href="https://redpacketsecurity.com/siemens-tecnom...">redpacketsecurity.com/siemens-tecnom...</a> #CVE #Vulnerability... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> |                             |                          |        |         | 2023-02-17 10:05:55 |
|  /r/netcve     | <a href="#">CVE-2023-24988</a>                                                                                                                                                                                                                                                       |                             |                          |        |         | 2023-02-14 12:38:42 |
| <a href="#">← Previous ID</a>                                                                  |                                                                                                                                                                                                                                                                                      |                             | <a href="#">Next ID→</a> |        |         |                     |