



# CVE-2020-26991

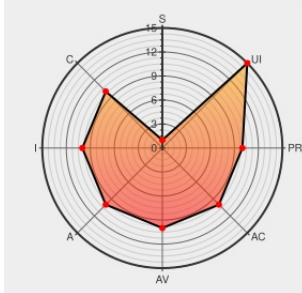
Published on: 01/12/2021 12:00:00 AM UTC

Last Modified on: 10/06/2022 07:42:00 PM UTC

## CVE-2020-26991

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



Certain versions of **Jt2go** from **Siemens** contain the following vulnerability:

A vulnerability has been identified in JT2Go (All versions < V13.1.0.2), Teamcenter Visualization (All versions < V13.1.0.2). Affected applications lack proper validation of user-supplied data when parsing ASM files. This could lead to pointer dereferences of a value obtained from untrusted source. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11899)

CVE-2020-26991 has been assigned by **S** productcert@siemens.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **S** **Siemens** - **JT2Go** version **All versions < V13.1.0.2**

Affected Vendor/Software: **S** **Siemens** - **Teamcenter Visualization** version **All versions < V13.1.0.2**

CVSS3 Score: **8.8 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</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>         |

CVSS2 Score: **6.8 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>PARTIAL</b>    | <b>PARTIAL</b>      |

CVE References

| Description                      | Tags                                                                                                                                        | Link                                                                                                                                                             |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                  | <a href="#">cert-portal.siemens.com</a><br><a href="#">application/pdf</a>                                                                  |  CONFIRM <a href="#">cert-portal.siemens.com/productcert/pdf/ssa-663999.pdf</a> |
| ZDI-21-053   Zero Day Initiative | <a href="#">Third Party Advisory</a><br><a href="#">VDB Entry</a><br><a href="#">www.zerodayinitiative.com</a><br><a href="#">text/html</a> |  MISC <a href="#">www.zerodayinitiative.com/advisories/ZDI-21-053/</a>          |
|                                  | <a href="#">cert-portal.siemens.com</a><br><a href="#">application/pdf</a>                                                                  |  MISC <a href="#">cert-portal.siemens.com/productcert/pdf/ssa-695540.pdf</a>    |
|                                  | <a href="#">Vendor Advisory</a><br><a href="#">cert-portal.siemens.com</a><br><a href="#">application/pdf</a>                               |  CONFIRM <a href="#">cert-portal.siemens.com/productcert/pdf/ssa-622830.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](mailto: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 | Jt2go                    | All     | All    | All     | All      |
| Application                                             | Siemens | Jt2go                    | All     | All    | All     | All      |
| Application                                             | Siemens | Teamcenter Visualization | All     | All    | All     | All      |
| Application                                             | Siemens | Teamcenter Visualization | All     | All    | All     | All      |
| cpe:2.3:a:siemens:jt2go:*:*:*:*:*.*:                    |         |                          |         |        |         |          |
| cpe:2.3:a:siemens:jt2go:*:*:*:*:*.*:                    |         |                          |         |        |         |          |
| cpe:2.3:a:siemens:teamcenter_visualization:*:*:*:*:*.*: |         |                          |         |        |         |          |
| cpe:2.3:a:siemens:teamcenter_visualization:*:*:*:*:*.*: |         |                          |         |        |         |          |

No vendor comments have been submitted for this CVE

## Social Mentions

| Source | Title | Posted (UTC) |
|--------|-------|--------------|
|--------|-------|--------------|

[← Previous ID](#)

Next ID→

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)