



CVE-2020-26985

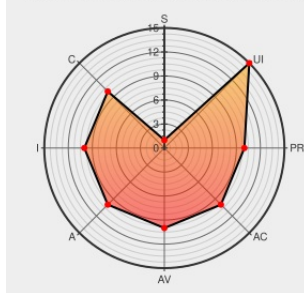
Published on: 01/12/2021 12:00:00 AM UTC

Last Modified on: 05/19/2021 04:06:57 PM UTC

CVE-2020-26985

[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), Teamcenter Visualization (All versions < V13.1.0). Affected applications lack proper validation of user-supplied data when parsing of RGB and SGI files. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11986, ZDI-CAN-11994)

CVE-2020-26985 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**

Affected Vendor/Software: **S** **Siemens** - **Teamcenter Visualization** version **All versions < V13.1.0**

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
ZDI-21-058 Zero Day Initiative	Third Party Advisory VDB Entry www.zerodayinitiative.com text/html	 MISC www.zerodayinitiative.com/advisories/ZDI-21-058/
ZDI-21-056 Zero Day Initiative	Third Party Advisory VDB Entry www.zerodayinitiative.com text/html	 MISC www.zerodayinitiative.com/advisories/ZDI-21-056/
	Vendor Advisory cert-portal.siemens.com application/pdf	 MISC cert-portal.siemens.com/productcert/pdf/ssa-622830.pdf

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	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:it2go:*:*:*:*:*:*:
```

```
cpe:2.3:a:siemens:teamcenter_visualization:*.*.*.*.*.*.*.*.:
```

```
cpe:2.3:a:siemens:teamcenter visualization:*.*.*.*.*.*.*.*
```

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

