

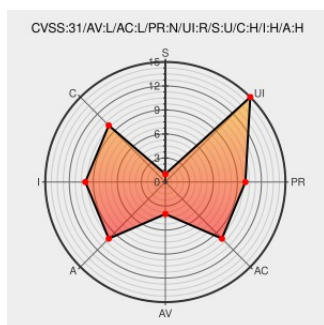


CVE-2021-44002

Published on: Not Yet Published

Last Modified on: 02/21/2023 06:34:00 PM UTC

CVE-2021-44002

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

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

A vulnerability has been identified in JT Open (All versions < V11.1.1.0), JT Utilities (All versions < V13.1.1.0), Solid Edge (All versions < V2023). The Jt1001.dll contains an out of bounds write past the end of an allocated structure while parsing specially crafted JT files.

This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15058, ZDI-CAN-19076, ZDI-CAN-19077)

CVE-2021-44002 has been assigned by **S** productcert@siemens.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **S** **Siemens** - **JT Open** version = **All versions < V11.1.1.0**

Affected Vendor/Software: **S** **Siemens** - **JT Utilities** version = **All versions < V13.1.1.0**

Affected Vendor/Software: **S** **Siemens** - **Solid Edge** version = **All versions < V2023**

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	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-22-006 Zero Day Initiative	www.zerodayinitiative.com text/html	 MISC www.zerodayinitiative.com/advisories/ZDI-22-006/
	cert-portal.siemens.com application/pdf	 MISC cert-portal.siemens.com/productcert/pdf/ssa-595101.pdf
	cert-portal.siemens.com application/pdf	 MISC cert-portal.siemens.com/productcert/pdf/ssa-936212.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.

Related QID Numbers

590730 Siemens JT2Go Multiple Vulnerabilities (ICSA-21-350-10)

590752 Siemens JT2Go and Teamcenter Visualization Multiple Vulnerabilities (ICSA-21-350-10)

590753 Siemens JT2Go and Teamcenter Visualization Multiple Vulnerabilities (ICSA-21-350-10)

Exploit/POC from Github

A vulnerability has been identified in JT Open (All versions < V11.1.1.0), JT Utilities (All versions < V13.1.1.0), S...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Siemens	Jt2go	All	All	All	All
Application	Siemens	Jt Open Toolkit	All	All	All	All
Application	Siemens	Jt Utilities	All	All	All	All
Application	Siemens	Solid Edge	All	All	All	All
Application	Siemens	Teamcenter Visualization	All	All	All	All

```
cpe:2.3:a:siemens:jt2go:*.*****:
```

```
cpe:2.3:a:siemens:jt_open_toolkit:*:*:*:*:*:
```

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

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-44002 : A vulnerability has been identified in JT2Go All versions < V13.2.0.5 , Teamcenter Visualization... twitter.com/i/web/status/1...	2021-12-14 12:15:40

[← Previous ID](#)[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)