

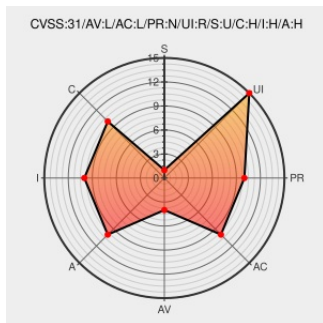


CVE-2022-3159

Published on: Not Yet Published

Last Modified on: 01/23/2023 06:33:00 PM UTC

CVE-2022-3159

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

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

The APDFL.dll contains a stack-based buffer overflow vulnerability that could be triggered while parsing specially crafted PDF files. This could allow an attacker to execute code in the context of the current process.

CVE-2022-3159 has been assigned by [ics-cert@hq.dhs.gov](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Siemens](#) - **JT2Go** version = 0

Affected Vendor/Software: [Siemens](#) - **Teamcenter Visualization V13.3** version = 0

Affected Vendor/Software: [Siemens](#) - **Teamcenter Visualization V14.0** version = 0

Affected Vendor/Software: [Siemens](#) - **Teamcenter Visualization V14.1** version = 0

Vulnerability Patch/Work Around

Siemens identified the following specific workaround and mitigation user can apply to reduce risk: * Do not open untrusted PDF files in JT2Go and Teamcenter Visualization. As a general security measure, Siemens recommends protecting network access to devices with appropriate mechanisms. To operate the devices in a protected IT environment, Siemens recommends configuring the environment according to Siemens' operational guidelines for industrial security <https://www.siemens.com/cert/operational-guidelines-industrial-security> and following the recommendations in the product manuals. Siemens also provides additional information on industrial security <https://www.siemens.com/industrialsecurity> . For further inquiries on security vulnerabilities in Siemens products, users should contact Siemens <https://www.siemens.com/cert/advisories> . For more information, see the associated Siemens security advisory SSA-360681 in HTML <https://cert-portal.siemens.com/productcert/html/ssa-360681.html> and CSAF <https://cert-portal.siemens.com/productcert/csaf/ssa-360681.json> .

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact

CVE References

Description	Tags	Link
Siemens Teamcenter Visualization and JT2Go CISA	www.cisa.gov text/html	 MISC www.cisa.gov/uscert/ics/advisories/icsa-22-349-15
	cert-portal.siemens.com application/json	 MISC cert-portal.siemens.com/productcert/csaf/ssa-360681.json
SSA-360681	cert-portal.siemens.com text/html	 MISC cert-portal.siemens.com/productcert/html/ssa-360681.html

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

591305 Siemens J2TGo Multiple Vulnerabilities (SSA-360681)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Siemens	Jt2go	All	All	All	All
Application	Siemens	Teamcenter Visualization	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-3159 : The APDFL.dll contains a stack-based buffer overflow vulnerability that could be triggered while pa... twitter.com/i/web/status/1...	2023-01-13 01:05:02
 /r/netcve	CVE-2022-3159	2023-01-13 02:38:45

[← Previous ID](#)

Next ID→

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](#)