



CVE-2022-2069

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-2069
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-20 17:15:00 UTC
Updated	2022-10-21 19:05:00 UTC
Description	The APDFL.dll in Siemens JT2Go prior to V13.3.0.5 and Siemens Teamcenter Visualization prior to V14.0.0.2 contains an c

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Siemens Datalogics File Parsing Vulnerability (Update A) CISA	CONFIRM	www.cisa.gov	
cert-portal.siemens.com/productcert/pdf/ssa-829738.pdf	CONFIRM	cert-portal.siemens.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Siemens reported this vulnerability to CISA.

Legacy QID Mappings

[591144](#) Siemens JT2go Datalogics File Parsing Vulnerability (SSA-829738,icsa-22-195-07)

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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