CVE-2022-42751

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-42751
State	PUBLIC
Assigner	help@fluidattacks.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-03 18:15:00 UTC
Updated	2022-11-04 15:12:00 UTC
Description	CandidATS version 3.0.0 allows an external attacker to elevate privileges in the application. This is possible because the ap

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Auieo	Candidats	3.0.0	All	All	All
Application	Auieo	Candidats	3.0.0	-	All	All

References

Reference	Source	Link	Tags
CandidATS 3.0.0 - CSRF to Privilege Escalation | Advisories | Fluid Attacks	MISC	fluidattacks.com	
Home - Candid ATS	MISC	candidats.net	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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