



CVE-2023-28857

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

Summary

CVE	CVE-2023-28857
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-27 18:15:00 UTC
Updated	2023-07-06 18:11:00 UTC
Description	Apereo CAS is an open source multilingual single sign-on solution for the web. Apereo CAS can be configured to use authentication...

Risk And Classification

Problem Types: CWE-522

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apereo	Central Authentication Service	All	All	All	All

References

Reference	Source	Link
CAS X.509 Vulnerability Disclosure – Apereo Community Blog	MISC	apereo.g
GHSL-2023-009: Credentials leaks for LDAP authentication in Apereo CAS - CVE-2023-28857 GitHub Security Lab	MISC	securityl
Release v6.6.6 · apereo/cas · GitHub	MISC	github.cc
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.

No vendor comments have been submitted for this CVE.

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

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