CVE-2015-1169

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

Summary

CVE	CVE-2015-1169
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-02-10 20:59:00 UTC
Updated	2015-02-11 19:47:00 UTC
Description	Apereo Central Authentication Service (CAS) Server before 3.5.3 allows remote attackers to conduct LDAP injection attacks

Risk And Classification

Problem Types: CWE-74

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
CAS-1429 Escape inputs into LDAP filter expressions. by serac · Pull Request #411 · apereo/cas · GitHub	CONFIR
[CAS-1429] Successful LDAP authentication with wildcard Login - JASIG Issue Tracker	CONFIR
Merge pull request #411 from serac/CAS-1429-ldap-filter-encoding · apereo/cas@7de61b4 · GitHub	CONFIR
Full Disclosure: CVE-2015-1169 - CAS Server 3.5.2 allows remote attackers to bypass LDAP authentication via crafted wildcards.	FULLDIS
CAS Server 3.5.2 LDAP Authentication Bypass ≈ Packet Storm	MISC
CVE Program record	CVE.OR
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report