



# CVE-2015-1169

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

## Summary

<b>CVE</b>	CVE-2015-1169
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-02-10 20:59:00 UTC
<b>Updated</b>	2015-02-11 19:47:00 UTC
<b>Description</b>	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	CONFIRMED
[CAS-1429] Successful LDAP authentication with wildcard Login - JASIG Issue Tracker	CONFIRMED
Merge pull request #411 from serac/CAS-1429-ldap-filter-encoding · apereo/cas@7de61b4 · GitHub	CONFIRMED
Full Disclosure: CVE-2015-1169 - CAS Server 3.5.2 allows remote attackers to bypass LDAP authentication via crafted wildcards.	FULLDISCLOSURE
CAS Server 3.5.2 LDAP Authentication Bypass ≈ Packet Storm	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

© [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](#)