



# CVE-2014-4172

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2014-4172
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-01-24 19:15:00 UTC
<b>Updated</b>	2023-11-07 02:20:00 UTC
<b>Description</b>	A URL parameter injection vulnerability was found in the back-channel ticket validation step of the CAS protocol in Jasig Ja

## Risk And Classification

### Problem Types: CWE-74

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Aperero</a>	<a href="#">.net Cas Client</a>	All	All	All	All
Application	<a href="#">Aperero</a>	<a href="#">.net Cas Client</a>	All	All	All	All
Application	<a href="#">Aperero</a>	<a href="#">Java Cas Client</a>	All	All	All	All
Application	<a href="#">Aperero</a>	<a href="#">Java Cas Client</a>	All	All	All	All
Application	<a href="#">Aperero</a>	<a href="#">Phpcas</a>	All	All	All	All
Application	<a href="#">Aperero</a>	<a href="#">Phpcas</a>	All	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	20	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	20	All	All	All

## References

Reference	Source	Link
phpCAS/ChangeLog at master · aperero/phpCAS · GitHub	MISC	<a href="#">github.cc</a>
Debian -- Security Information -- DSA-3017-1 php-cas	MISC	<a href="#">www.dek</a>
#759718 - php-cas needs to urlencode all tickets (CVE-2014-4172) - Debian Bug report logs	MISC	<a href="#">bugs.dek</a>
[cas-user] CAS Client Security Vulnerability CVE-2014-4172		<a href="#">www.ma</a>

[SECURITY] Fedora 20 Update: cas-client-3.3.3-1.fc20	MISC	<a href="#">lists.fedo</a>
IBM X-Force Exchange	MISC	<a href="#">exchang</a>
URL Encode ticket parameter when presented for validation. by serac · Pull Request #125 · apereo/phpCAS · GitHub	MISC	<a href="#">github.cc</a>
NETC-60 URL encode ticket parameter value. · apereo/dotnet-cas-client@f0e0300 · GitHub	MISC	<a href="#">github.cc</a>
1131350 – (CVE-2014-4172) CVE-2014-4172 cas-client: Bypass of security constraints via URL parameter injection	MISC	<a href="#">bugzilla.r</a>
[cas-user] CAS Client Security Vulnerability CVE-2014-4172	MISC	<a href="#">www.ma</a>
CASC-228 URL Encode Paramaters Passed to Server via Validate · apereo/java-cas-client@ae37092 · GitHub	MISC	<a href="#">github.cc</a>
[CASC-228] CVE-2014-4172 URL Encode Parameters Passed to Validate Endpoints - Jira	MISC	<a href="#">issues.ja</a>
CVE Program record	CVE.ORG	<a href="#">www.cve</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.g</a>

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](#)