



CVE-2012-1104

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

Summary

CVE	CVE-2012-1104
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-12-05 18:15:00 UTC
Updated	2019-12-30 12:59:00 UTC
Description	A Security Bypass vulnerability exists in the phpCAS 1.2.2 library from the jasig project due to the way proxying of services

Risk And Classification

Problem Types: CWE-269

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Aperoo	Phpcas	1.2.2	All	All	All
Application	Aperoo	Phpcas	1.2.2	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All

References

Reference	Source	L
801343 – (CVE-2012-1104) CVE-2012-1104 php-pear-CAS: Improper management of service proxying	MISC	b
web/lib/CAS/CAS-1.3.5/docs/ChangeLog · b18bcde090dc38fc968a0b1e38d1dab08b8c369e · Jakub Kalnik / sixmon · GitLab	CONFIRM	g
phpCAS Proxy Authorization Security Bypass Vulnerability	MISC	w
CVE-2012-1104	MISC	s
oss-security - Re: CVE Requests for phpCAS	MISC	w
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

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](#)