



# CVE-2010-2795

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

## Summary

|                 |                                                                                                                               |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2010-2795                                                                                                                 |
| State           | PUBLISHED                                                                                                                     |
| Assigner        | redhat                                                                                                                        |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                  |
| Published       | 2010-08-05 18:17:57 UTC                                                                                                       |
| Updated         | 2026-04-29 01:13:23 UTC                                                                                                       |
| Description     | phpCAS before 1.1.2 allows remote authenticated users to hijack sessions via a query string containing a crafted ticket value |

## Risk And Classification

**Primary CVSS:** v2.0 4 from nvd@nist.gov

AV:N/AC:L/Au:S/C:N/I:P/A:N

**Problem Types:** CWE-20 | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:L/Au:S/C:N/I:P/A:N

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor           | Product | Version | Update | Edition | Language |
|-------------|------------------|---------|---------|--------|---------|----------|
| Application | Joachim Fritschi | Phpcas  | 0.2     | All    | All     | All      |

|             |                                  |                        |        |     |     |     |
|-------------|----------------------------------|------------------------|--------|-----|-----|-----|
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.3    | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.3.1  | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.3.2  | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.4    | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.4.1  | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.4.10 | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.4.11 | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.4.12 | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.4.13 | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.4.14 | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.4.15 | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.4.16 | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.4.17 | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.4.18 | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.4.19 | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.4.2  | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.4.20 | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.4.21 | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.4.22 | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.4.23 | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.4.3  | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.4.4  | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.4.5  | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.4.6  | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.4.7  | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.4.8  | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.4.9  | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.5.0  | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.5.1  | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 0.6.0  | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 1.0.0  | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 1.0.1  | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | 1.1.0  | All | All | All |
| Application | <a href="#">Joachim Fritschi</a> | <a href="#">Phpcas</a> | All    | All | All | All |

| Source                                                                                                                                        | Vendor | Product | Version      | Platforms     |
|-----------------------------------------------------------------------------------------------------------------------------------------------|--------|---------|--------------|---------------|
| CNA                                                                                                                                           | Na     | N/a     | affected n/a | Not specified |
| References                                                                                                                                    |        |         |              |               |
| Reference                                                                                                                                     |        |         |              |               |
| [SECURITY] Fedora 13 Update: glpi-0.72.4-3.svn11497.fc13                                                                                      |        |         |              |               |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                                                              |        |         |              |               |
| forge.indepnet.net/projects/glpi/repository/revisions/12601                                                                                   |        |         |              |               |
| [PHPCAS-61] When already logged in, providing a new well formed ticket value in url will only cause the session id to change, without any val |        |         |              |               |
| [SECURITY] Fedora 12 Update: php-pear-CAS-1.1.2-1.fc12                                                                                        |        |         |              |               |
| Debian update for moodle - Secunia.com                                                                                                        |        |         |              |               |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                                                              |        |         |              |               |
| Fedora update for php-pear-CAS - Advisories - Community                                                                                       |        |         |              |               |
| Debian -- Security Information -- DSA-2172-1 moodle                                                                                           |        |         |              |               |
| GLPI phpCAS Multiple Vulnerabilities - Secunia.com                                                                                            |        |         |              |               |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                                                              |        |         |              |               |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                                                              |        |         |              |               |
| IBM X-Force Exchange                                                                                                                          |        |         |              |               |
| phpCAS Session Hijacking and Cross-Site Scripting Vulnerabilities - Advisories - Community                                                    |        |         |              |               |
| [SECURITY] Fedora 13 Update: php-pear-CAS-1.1.2-1.fc13                                                                                        |        |         |              |               |
| Confluence                                                                                                                                    |        |         |              |               |
| phpCAS Service Ticket Validation Session Hijacking Vulnerability                                                                              |        |         |              |               |
| [SECURITY] Fedora 12 Update: glpi-0.72.4-3.svn11497.fc12                                                                                      |        |         |              |               |
| Fedora update for glpi - Secunia.com                                                                                                          |        |         |              |               |
| CVE Program record                                                                                                                            |        |         |              |               |
| NVD vulnerability detail                                                                                                                      |        |         |              |               |
| No vendor comments have been submitted for this CVE.                                                                                          |        |         |              |               |
| There are currently no legacy QID mappings associated with this CVE.                                                                          |        |         |              |               |

[site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)