



# CVE-2010-3691

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

## Summary

<b>CVE</b>	CVE-2010-3691
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2010-10-07 21:00:00 UTC
<b>Updated</b>	2019-12-30 12:59:00 UTC
<b>Description</b>	PGTStorage/pgt-file.php in phpCAS before 1.1.3, when proxy mode is enabled, allows local users to overwrite arbitrary files

## Risk And Classification

### Problem Types: CWE-59

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Aperero</a>	<a href="#">Phpcas</a>	0.2	All	All	All
Application	<a href="#">Aperero</a>	<a href="#">Phpcas</a>	0.3	All	All	All
Application	<a href="#">Aperero</a>	<a href="#">Phpcas</a>	0.3.1	All	All	All
Application	<a href="#">Aperero</a>	<a href="#">Phpcas</a>	0.3.2	All	All	All
Application	<a href="#">Aperero</a>	<a href="#">Phpcas</a>	0.4	All	All	All
Application	<a href="#">Aperero</a>	<a href="#">Phpcas</a>	0.4.1	All	All	All
Application	<a href="#">Aperero</a>	<a href="#">Phpcas</a>	0.4.10	All	All	All
Application	<a href="#">Aperero</a>	<a href="#">Phpcas</a>	0.4.11	All	All	All
Application	<a href="#">Aperero</a>	<a href="#">Phpcas</a>	0.4.12	All	All	All
Application	<a href="#">Aperero</a>	<a href="#">Phpcas</a>	0.4.13	All	All	All
Application	<a href="#">Aperero</a>	<a href="#">Phpcas</a>	0.4.14	All	All	All
Application	<a href="#">Aperero</a>	<a href="#">Phpcas</a>	0.4.15	All	All	All
Application	<a href="#">Aperero</a>	<a href="#">Phpcas</a>	0.4.16	All	All	All
Application	<a href="#">Aperero</a>	<a href="#">Phpcas</a>	0.4.17	All	All	All
Application	<a href="#">Aperero</a>	<a href="#">Phpcas</a>	0.4.18	All	All	All
Application	<a href="#">Aperero</a>	<a href="#">Phpcas</a>	0.4.19	All	All	All
Application	<a href="#">Aperero</a>	<a href="#">Phpcas</a>	0.4.20	All	All	All

Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.4.21	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.4.22	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.4.23	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.4.8	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.4.9	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.5.0	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.5.1	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.6.0	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	1.0.0	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	1.0.1	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	1.1.0	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	1.1.1	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.2	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.3	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.3.1	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.3.2	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.4	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.4.1	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.4.10	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.4.11	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.4.12	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.4.13	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.4.14	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.4.15	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.4.16	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.4.17	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.4.18	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.4.19	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.4.20	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.4.21	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.4.22	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.4.23	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.4.8	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.4.9	All	All	All
Application	<a href="#">Aperio</a>	<a href="#">Phpcas</a>	0.5.0	All	All	All

Application	<a href="#">Aperoo</a>	<a href="#">Phpcas</a>	0.5.1	All	All	All
Application	<a href="#">Aperoo</a>	<a href="#">Phpcas</a>	0.6.0	All	All	All
Application	<a href="#">Aperoo</a>	<a href="#">Phpcas</a>	1.0.0	All	All	All
Application	<a href="#">Aperoo</a>	<a href="#">Phpcas</a>	1.0.1	All	All	All
Application	<a href="#">Aperoo</a>	<a href="#">Phpcas</a>	1.1.0	All	All	All
Application	<a href="#">Aperoo</a>	<a href="#">Phpcas</a>	1.1.1	All	All	All
Application	<a href="#">Aperoo</a>	<a href="#">Phpcas</a>	All	All	All	All

## References

Reference	Source	Link
[PHPCAS-80] Proxy tickets and writing on disk needs more checks - Jira	CONFIRM	<a href="#">issues</a>
#495542 - ITP: php-cas -- Central Authentication Service client library in php - Debian Bug report logs	CONFIRM	<a href="#">bugs.d</a>
FishEye: changeset 21538	CONFIRM	<a href="#">develo</a>
forge.indepnet.net/projects/glpi/repository/revisions/12601	CONFIRM	<a href="#">forge.i</a>
phpCAS Proxy Mode Multiple Security Vulnerabilities	BID	<a href="#">www.s</a>
oss-security - CVE request - phpCAS: prevent symlink attacks, directory traversal and XSS during a proxy callback	MLIST	<a href="#">www.o</a>
Debian -- Security Information -- DSA-2172-1 moodle	DEBIAN	<a href="#">www.d</a>
Fedora update for php-pear-CAS - Secunia.com	SECUNIA	<a href="#">secuni</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="#">www.v</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="#">www.v</a>
GLPI phpCAS Multiple Vulnerabilities - Secunia.com	SECUNIA	<a href="#">secuni</a>
[SECURITY] Fedora 12 Update: glpi-0.72.4-3.svn11497.fc12	FEDORA	<a href="#">lists.fe</a>
Fedora update for glpi - Secunia.com	SECUNIA	<a href="#">secuni</a>
Debian update for moodle - Secunia.com	SECUNIA	<a href="#">secuni</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="#">www.v</a>
oss-security - Re: CVE request - phpCAS: prevent symlink attacks, directory traversal and XSS during a proxy callback	MLIST	<a href="#">www.o</a>
oss-security - Re: CVE request - phpCAS: prevent symlink attacks, directory traversal and XSS during a proxy callback	MLIST	<a href="#">www.o</a>
[SECURITY] Fedora 13 Update: php-pear-CAS-1.1.3-1.fc13	FEDORA	<a href="#">lists.fe</a>
[SECURITY] Fedora 12 Update: php-pear-CAS-1.1.3-1.fc12	FEDORA	<a href="#">lists.fe</a>
[SECURITY] Fedora 13 Update: glpi-0.72.4-3.svn11497.fc13	FEDORA	<a href="#">lists.fe</a>
CVE Program record	CVE.ORG	<a href="#">www.c</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nis</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](#)