



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 23 août 2010
N° CERTA-2010-AVI-398

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans phpCAS

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-398>

Gestion du document

Référence	CERTA-2010-AVI-398
Titre	Vulnérabilités dans phpCAS
Date de la première version	23 août 2010
Date de la dernière version	–
Source(s)	Notes de la version 1.1.2 de phpCAS
Pièce(s) jointe(s)	Aucune

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Contournement de la politique de sécurité ;
- injection de code indirecte à distance.

2 Systèmes affectés

phpCAS versions 1.1.1 et antérieures.

3 Résumé

Deux vulnérabilités dans *phpCAS* permettent de réaliser une injection de code indirecte et de détourner une session.

4 Description

Deux vulnérabilités ont été découvertes dans *phpCAS* :

- un utilisateur déjà connecté peut produire des tickets qui seront assignés à une autre session sans validation (CVE-2010-2795) ;

- une injection de code indirecte est possible via les URL de *callback* lorsque le mode *proxy* est activé (CVE-2010-2796).

5 Solution

Mettre *phpCAS* à jour en version 1.1.2.

6 Documentation

- Notes de la version 1.1.2 de *phpCAS* :
<https://wiki.jasig.org/display/CASC/phpCAS+ChangeLog>
- Référence CVE CVE-2010-2795 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2795>
- Référence CVE CVE-2010-2796 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2796>

Gestion détaillée du document

23 août 2010 version initiale.