Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 octobre 2010
N° CERTA-2010-AVI-477

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans phpCAS

Gestion du document

Référence	CERTA-2010-AVI-477
Titre	Multiples vulnérabilités dans phpCAS
Date de la première version	08 octobre 2010
Date de la dernière version	–
Source(s)	Notes de la version 1.1.3 de phpCAS du 05 octobre 2010
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

- Exécution de code arbitraire à distance ;
- élévation de privilèges ;
- injection de code indirecte à distance.

2 Systèmes affectés

phpCAS versions 1.1.2 et antérieures.

3 Résumé

De multiples vulnérabilités dans *phpCAS* permettent de réaliser une injection de code indirecte, d'élever les privilèges ou d'exécuter du code arbitraire à distance.

4 Description

De multiples vulnérabilités ont été découvertes dans *phpCAS* :

- de multiples injections de code indirectes sont possibles lorsque le mode proxy est activé (CVE-2010-3690) ;

- une faille dans le fichier `PGTStorage/pgt-file.php` permet, lorsque le mode proxy est activé, une élévation de privilèges (CVE-2010-3691) ;
- une traversée de répertoires est possible via le fichier `client.php` lorsque le mode proxy est activé. Cette vulnérabilité permet notamment de créer ou d'écraser des fichiers (CVE-2010-3692).

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Notes de la version 1.1.3 de phpCAS du 05 octobre 2010 :
  https://wiki.jasig.org/display/CASC/phpCAS+ChangeLog
- Référence CVE CVE-2010-3690 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3690
- Référence CVE CVE-2010-3691 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3691
- Référence CVE CVE-2010-3692 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3692

Gestion détaillée du document

08 octobre 2010 version initiale.