Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 septembre 2007
N° CERTA-2007-AVI-393

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans CAS

Gestion du document

Référence	CERTA-2007-AVI-393
Titre	Vulnérabilité dans CAS
Date de la première version	07 septembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité ESUP-2007-AVI-002 du 03 septembre 2007
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

Attaques de type *cross-site scripting*.

2 Systèmes affectés

Tous les serveurs CAS distribués par l'université de Yale jusqu'à la version 2.0.12 incluse :

– `cas-server` 2.x.

Toutes les distributions `esup-cas-quick-start` et `esup-cas-server` du consortium ESUP-Portail jusqu'à la version 2.0.7 incluse :

– `esup-cas-quick-start` 1.0.x et 2.0.x ;
– `esup-cas-server` 1.0.x et 2.0.x.

3 Résumé

Une vulnérabilité dans le serveur `CAS` permet de réaliser des attaques de type *cross-site scripting*.

4 Description

Une vulnérabilité a été découverte dans le serveur `CAS`. Elle permet, en passant certaines valeurs au paramètre `service` de la page d'authentification, d'accéder au `cookie` de session.

5 Solution

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

6 Documentation

– Bulletin de sécurité du consortium ESUP-Portail ESUP-2007-AVI-002 du 03 septembre 2007 : http://www.esup-portail.org/AvisSecurite

Gestion détaillée du document

07 septembre 2007 version initiale.