

# ESUP-2007-AVI-002 - Vulnérabilité dans le service d'authentification CAS

## Utilisation et diffusion de ce document

Les avis de sécurité du consortium ESUP-Portail portent sur des vulnérabilités des logiciels diffusés par le consortium. Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit, pour des raisons évidentes de sécurité des Systèmes d'Information de tous les établissements du consortium ESUP-Portail.

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Objet                       | Vulnérabilité dans le service d'authentification CAS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Référence                   | ESUP-2007-AVI-002                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Date de la première version | 4 juillet 2007                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Date de la dernière version | 3 septembre 2007                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Source                      | interne                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Diffusion de cette version  | Publique                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Historique                  | <ul style="list-style-type: none"><li>• 4 juillet 2007 : réception de la vulnérabilité par la coordination technique du consortium ESUP-Portail</li><li>• 5 juillet 2007 : validation de la vulnérabilité par le consortium ESUPPortail (Pascal AUBRY, Vincent MATHIEU, Julien MARCHAL)</li><li>• 6 juillet 2007 : concertation avec les correspondants sécurité du consortium JASIG (security@jasig.org)</li><li>• 9 juillet 2007 : validation de la vulnérabilité par l'université de Yale (Howard GILBERT)</li><li>• 25 juillet 2007 : écriture du correctif et envoi à la coordination technique ESUP-Portail pour test (Howard GILBERT)</li><li>• 16 août 2007 : retour négatif à Howard GILBERT (Raymond BOURGES)</li><li>• 20 août 2007 : mise au point du correctif final et envoi à la coordination technique ESUP-Portail pour test (Howard GILBERT)</li><li>• 22 août 2007 : validation du correctif final et intégration dans les distribution esup-cas-server et esup-cas-quick-start (Pascal AUBRY)</li><li>• 23 août 2007 : diffusion simultanée par l'université de Yale et le consortium ESUP-Portail de l'avis à leurs correspondants sécurité</li><li>• 3 septembre 2007 : annonce publique de la vulnérabilité</li></ul> |
| Pièces jointes              | <a href="#">ESUP-2007-AVI-002-COR.zip</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Risque

Usurpation de l'identité des utilisateurs.

## 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
- esup-cas-quick-start 2.0.x
- esup-cas-server 1.0.x
- esup-cas-server 2.0.x

## Résumé

Une vulnérabilité dans le serveur CAS permet via une attaque de type Cross Site Scripting (XSS) d'usurper l'identité des utilisateurs.

## Description

Il est possible, en passant certaines valeurs au paramètre service de la page d'authentification du serveur CAS, de voler le cookie d'authentification (Ticket Granting Cookie)

## Solution

L'administrateur du serveur CAS devra utiliser l'une des trois méthodes ci-dessous.

Méthode 1 : faire une mise à jour complète du serveur

**Méthode 1a** (pour les utilisateurs de la distribution cas-server de l'université de Yale) : utiliser la version 2.0.12c, incluse dans le correctif [ESUP-2007-AVI-002-COR.zip](#).

**Méthode 1b** (pour les utilisateurs d'une des distributions esup-cas-server ou esup-cas-quickstart du consortium ESUP-Portail) : utiliser la version 2.1.2, téléchargeable sur <http://esupcasgeneric.sourceforge.net>.

## Méthode 2 : modifier le code Java

Ecraser la classe edu.yale.its.tp.cas.servlet.Login.java en la remplaçant par celle trouvée dans le correctif [ESUP-2007-AVI-002-COR.zip](#).

## Méthode 3 : modifier le code JSP

Modifier la page /web/goService.jsp pour supprimer les caractères '<' et '>' du paramètre service (un exemple de page JSP goService.jsp est inclus dans le correctif [ESUP-2007-AVI-002-COR.zip](#)).