ESUP-2009-AVI-002 - Vulnérabilité dans esup-commons

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 esup-commons
Référence	ESUP-2009-AVI-002
Date de la première version	11 mars 2009
Date de la dernière version	11 mars 2009
Source	The Apache Software Foundation
Diffusion de cette version	Publique
Historique	• 9 mars 2009 : découverte de la vulnérabilité dans le ChangeLog de Tomahawk • 11 mars 2009 : diffusion de la version 0.21.0 apportant le correctif (Pascal Aubry)
Pièces jointes	aucune.

Risque

Usurpation de l'identité des utilisateurs par récupération des identifiants de session.

Systèmes affectés

- Toutes les applications basées sur esup-commons jusqu'à la version 0.20.7.

Description

esup-commons utilise les extensions de Apache MyFaces proposées par la bibliothèque Tomahawk. La version 1.1.5 de cette librairie, utilisée par esup-commons depuis sa création, comporte un trou de sécurité important permettant l'injection de code Javascript arbitraire.

Les possibilités d'attaque par Cross Site Scripting incluent notamment la capture de l'identifiant de session, autorisant alors l'usurpation de l'identité de l'utilisateur, elles sont décrites en détail sur le site de iDefense Labs.

Solution

La version 0.21.0 embarque la version 1.1.6 de la bibliothèque Tomahawk qui corrige la vulnéraiblité (cf TOMAHAWK-983).

Il est recommandé à tous les mainteneurs d'applications basées sur esup-commons d'effectuer la mise à jour vers la version 0.21.0 ou ultérieure dès que possible.

Liens

- esup-commons - Framework de développement