ESUP-2009-AVI-001 - Vulnérabilité dans esup-helpdesk

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-helpdesk
Référence	ESUP-2009-AVI-001
Date de la première version	14 janvier 2009
Date de la dernière version	14 janvier 2009
Source	Université de Rennes 1
Diffusion de cette version	Publique
Historique	• 12 janvier 2009 : réception de la vulnérabilité • 13 janvier 2009 : validation de la vulnérabilité (Pascal Aubry) • 14 janvier 2009 : diffusion de la version 3.16.0 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 distributions esup-helpdesk de 3.0.0 à 3.15.2

Résumé

esup-helpdesk utilise FCK Editor pour l'entrée WYSIWYG des actions sur les tickets et l'édition des FAQs. Le code HTML entré de cette manière est ensuite affiché directement à l'utilisateur dans l'historique des tickets et dans les FAQs.

Description

- En version 3.0.0 à 3.15.2, en chargeant une page utilisant FCK editor et en désactivant Javascript, il est possible d'entrer du code arbitraire dans la base de données, en utilisant par exemple les balises HTML <script> ou <iframe>. Ce code est alors exécuté lors des affichages ultérieurs.
- En version 3.14.5 à 3.15.2, suite à une mauvaise mise à jour de FCK editor (passage de la version 1.7.26 à 1.8), il est possible d'entrer du code arbitraire sans même désactiver Javascript.

Les possibilités d'attaque par le code Javascript incluent notamment la capture de l'identifiant de session, autorisant alors l'usurpation de l'identité de l'utilisateur.

Solution

La version 3.16.0 :

- supprime les balises indélicates du code entré par les utilisateurs avant stockage en base de données ;
- supprime le code indélicat entré dans la base de données en utilisant une version antérieure.

Même s'il est possible de tracer l'injection de code (toutes les actions sont nominatives dans l'application), il est très fortement recommandé d'effectuer la mise à jour vers la version 3.16.0 ou ultérieure dès que possible.

Liens

- Téléchargement de esup-helpdesk : http://helpdesk.esup-portail.org
- Historique de l'application : ChangeLog