ESUP-2010-AVI-001 - Vulnérabilité dans le canal annuaire

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 canal Annuaire
Référence	ESUP-2010-AVI-001
Date de la première version	4 mars 2010
Date de la dernière version	8 mars 2010
Source	listes de diffusion supann-utilisateurs et esup-utilisateurs
Diffusion de cette version	Publique
Historique	• 2 mars 2010 : découverte et diffusion de la vulnérabilité dans les listes supann-utilisateurs et esup-utilisateurs • 5 mars 2010 : diffusion de la version 3.2 du canal qui corrige la vulnérabilité • 5 mars 2010 : diffusion de l'avis de sécurité aux correspondants sécurité du consortium ESUP-Portail • 6 mars 2010 : diffusion de la version 3.2.1 qui corrige un problème de déploiement du canal • 8 mars 2010 : avis public, avec annonce sur différentes listes
Pièces jointes	aucune.

Risque

Récupération automatique d'adresses électroniques, ou d'autre informations d'annuaire non contrôlées.

Systèmes affectés

- Toutes les distributions du canal annuaire, jusque la version 3.1 incluse.

Description

Un accès direct en mode anonyme à une fiche utilisateur (URL du genre http://ent.univ.fr/Guest?uP_fname=annu_public&id=toto) ne contrôle pas les restrictions indiquées dans le fichier de configuration, et permet l'accès à des informations d'annuaire qui ne devraient pas être accessibles.

Solution

La version 3.2.1 du canal annuaire corrige les problèmes identifiés.

Il est fortement recommandé d'effectuer la mise à jour vers la version 3.2.1 ou ultérieure très rapidement.

En cas d'impossibilité de mise à jour rapide de ce canal, et vu la divulgation publique du problème, il est fortement conseillé de positionner la propriété **max Entries** de la balise **request** des annuaires publics à une valeur très faible.

Liens

- Téléchargement du canal annuaire : http://sourcesup.cru.fr/frs/?group_id=208