ESUP-2009-AVI-004 - Vulnérabilité dans uPortal

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 uPortal
Référence	ESUP-2009-AVI-004
Date de la première version	10 décembre 2009
Date de la dernière version	10 décembre 2009
Source	liste de diffusion uportal-user du consortium JASIG
Diffusion de cette version	Publique
Historique	• 8 décembre 2009 : réception de la vulnérabilité • 10 décembre 2009 : diffusion de l'avis de sécurité aux correspondants sécurité du consortium ESUP-Portail (Julien Marchal)

Risque

Injection SQL

Systèmes affectés

- Toutes les distributions uPortal depuis la version 3.X, 2.6
- Toutes les distributions uPortal-esup (basées sur uPortal 2.6 et 3.1)

Résumé

La vulnérabilité n'est pas considéré comme grave parce qu'elle n'est accessible que via l'interface Channel Manager qui est limité aux administrateurs de portail.
Dans une installation uPortal normal, il n'y a aucun moyen pour un utilisateur non administrateur d'exécuter le code concerné.

Solution

Pour la version 2.6 appliquer le patch fournit en fichier joint : RDBMChannelRegistryStore.java.patch

De nouveau package esup-dlm-2.6 sont disponibles : a partir de la version esup-2.6-esup-2.0.6.tar.gz et esupdev-2.6-esup-2.0.6.tar.gz (http://sourcesup.cru.fr/frs/?group_id=173

> **Solution pour uPortal 3.X**
>
> Dans le cas d'une version 3.X étant donné ça nouveauté, le nouveau package incluera la patch.

Liens

- Le ticket JIRA montrant la vulnérabilité : http://www.ja-sig.org/issues/browse/UP-2515 http://www.ja-sig.org/issues/browse/UP-2088

[uportal-user] uPortal Security Announcement

by Eric Dalquist <eric.dalquist@doit.wisc.edu>

December 08th 2009

A SQL injection vulnerability was reported that affects all released versions of uPortal.
The vulnerability is not considered severe as it is only accessible via the Channel Manager interface which is restricted to portal administrators. In a standard uPortal installation there is no way for an anonymous or non-administrative user to execute the affect code.
Security patch releases uPortal 2.6.1.1and 2.5.3.2have been put out. The bug is fixed in the 3.1.2 and3.0.5releases which came out today. The details of the bug are documented in Jira issue: http://www.ja-sig.org/issues/browse/UP-2515
For those that cannot upgrade to a released version they are encouraged to apply a patch for the issue. Version specific patches are linked below:
uPortal 2.5: http://developer.jasig.org/source/rdiff/jasigsvn?csid=47293&u&N
uPortal 2.6: http://developer.jasig.org/source/rdiff/jasigsvn?csid=47294&u&N
uPortal 3.0: http://developer.jasig.org/source/rdiff/jasigsvn?csid=47295&u&N
uPortal 3.1: http://developer.jasig.org/source/rdiff/jasigsvn?csid=47296&u&N
Thank you,
-Eric Dalquist