Avis de sécurité 2007-004

Objet	Vulnérabilité dans esup-webdav-srv
Référence	ESUP-2007-AVI-004
Date de la première version	8 novembre 2007
Date de la dernière version	27 novembre 2007
Source	liste de diffusion slide-user@jakarta.apache.org du projet APACHE
Diffusion de cette version	**Publique**
Historique	2 novembre 2007 : réception de la vulnérabilité 5 novembre 2007 : validation de la vulnérabilité sur le package esup-webdav-srv distribué par le consortium ESUP-Portail (Vincent Bonamy et Raymond Bourges) 5 novembre 2007 : constatation que le patch proposé par le commiter slide réduit les fonctionnalités du produit sur une commande WebDAV de type LOCK (Vincent Bonamy et Raymond Bourges) 5 novembre 2007 : constatation que la faille de sécurité existe aussi sur une commande WebDAV de type PROPPATCH et n'est pas corrigée par le patch proposé par le commiter Slide (Vincent Bonamy et Raymond Bourges) 6 novembre 2007 : recherche d'une solution de patch ne limitant pas les fonctionnalités du produit et comblant la faille pour les commandes LOCK et PROPPATCH (Vincent Bonamy et Raymond Bourges) 8 novembre 2007 : développement du patch (Raymond Bourges) 8 novembre 2007 : validation du correctif (Vincent Bonamy et Raymond Bourges) 8 novembre 2007 : mise en ligne d'un nouveau correctif sous forme d'un patch pour la version 3.5 et d'une nouvelle version RC5 pour la version 5.2 9 novembre 2007 : envoi du correctif aux correspondants sécurité du consortium ESUP-Portail (après relecture par Pascal AUBRY) 27 novembre 2007 : annonce publique de la vulnérabilité par les consortiums ESUP-Portail
Pièces jointes	**`ESUP-2007-AVI-004-COR.zip`**

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.

Pour plus de renseignements : ***contact-tech@esup-portail.org***

Risque

Possibilité de lire à distance un fichier sur le serveur Unix ou Windows faisant tourner le serveur esup-webdav-srv.

Systèmes affectés

- Toutes les versions de esup-webdav-srv

Résumé

Exploitation d'une faille liée à l'utilisation d'une *ENTITY* de type *SYSTEM* dans une commande formulée en XML.

Description

Avec une commande LOCK ou PROPPATCH contenant une requête XML avec une *ENTITY* de type *SYSTEM* un pirate peut obtenir en réponse le fichier pointé par cette *ENTITY*. Il est donc possible de lire n'importe quel fichier du serveur pour lequel l'utilisateur, propriétaire du processus tomcat faisant tourner le serveur WebDAV, a un droit en lecture. A noter que les commandes LOCK ou PROPPATCH ne peuvent être exécutées que sur des ressources WebDAV pour lesquels on a un droit en écriture ce qui n'est généralement possible que pour des personnes pouvant s'identifier sur le serveur WebDAV.

Solution

Pour un serveur en version 3.5

Si vous ne décidez pas encore de passer sur une version 5.2 :

1. Stopper le serveur
2. A partir des classes contenues dans le correctif **`ESUP-2007-AVI-004-COR.zip`** copier `DummyEntityResolver.java` dans le répertoire `src/slide-update/src/webdav/server/org/apache/slide/webdav/sax` de votre répertoire d'installation du serveur WebDAV (le répertoire final `sax` est à créer)
3. A partir des classes contenues dans le correctif **`ESUP-2007-AVI-004-COR.zip`** copier `AbstractWebdavMethod.java` dans le répertoire `src/slide-update/src/webdav/server/org/apache/slide/webdav/method` de votre répertoire d'installation du serveur WebDAV
4. NE PAS OUBLIER : faire un `ant init`
5. faire un ant deploy
6. Relancer le serveur

Pour un serveur en version 5.2

1. Mettre à jour avec la version 5.2RC5 disponible sur sourcesup : http://sourcesup.cru.fr/frs/?group_id=207

Warning: Security-Bug in Slide
<ozeigermann@apache.org>
02/11/2007 09:26

```
Folks!

As described here

http://www.milw0rm.com/exploits/4567

there is a security bug in the current Slide release. Using the LOCK
methode it is possible to display content from your local file system.
This works by passing over literate XML that contains entities that
refer to your local file system.

AFAIK this can not be prevented by the XML implementation Slide uses (JDOM).

A quick fix would be to disable the LOCK method in the web.xml by
commenting it out or removing it.

I have also committed a patched LockMethod.java that does not return
literate XML at all. This may cause trouble with the owner filed that
some clients require, but it is the best I can do for now.

It is checked in in the Slide 2.1 release branch and in the HEAD
branch. For existing Slide 2.1 installations it would suffice to check
out, compile and replace the LockMethod class. You can do so by
copying it in the the WEB-INF/class folder including all package
directories.

If you grant outside access to your Slide WebDAVServer be sure to take
care of this bug.

Cheers

Oliver
```