Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 22 juin 2006
N° CERTA-2005-AVI-490-005

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sur le module mod_imap d'Apache

Conditions d'utilisation de ce document : `http://www.certa.ssi.gouv.fr/certa/apropos.html`
Dernière version de ce document : `http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-490`

Gestion du document

Référence	CERTA-2005-AVI-490-005
Titre	Vulnérabilité sur le module mod_imap d'Apache
Date de la première version	15 décembre 2005
Date de la dernière version	22 juin 2006
Source(s)	Bulletins de sécurité Apacheweek
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Elévation de privilèges.

2 Systèmes affectés

- Apache versions 1.3.0 à 1.3.34 ;
- Apache versions 2.0.35 à 2.0.55 ;

3 Résumé

Une vulnérabilité de type « cross site scripting » est présente dans le module `mod_imap` d'Apache. Cette vulnérabilité peut être utilisée par un utilisateur mal intentionné pour faire exécuter un script par le navigateur d'un utilisateur consultant le site vulnérable..

4 Description

Le module `mod_imap` est le module chargé de prendre en charge les fichiers au format `.map`.

Une vulnérabilité dans la directive `Referer` du module `mod_imap` peut être exploitée par un utilisateur mal intentionné pour faire exécuter un script par le navigateur d'un utilisateur tierce à partir d'un site vulnérable.

5 Solution

Les corrections de cette vulnérabilité sont effectuées dans les versions 1.3.35-dev et 2.0.56-dev d'Apache.

6 Documentation

- Site internet pour le module mod_imap :
  http://httpd.apache.org/docs/1.3/mod/mod_imap.html
- Bulletin de sécurité pour les versions 2.0.x d'Apache :
  http://httpd.apache.org/security/vulnerabilities_20.html
- Bulletin de sécurité pour les versions 1.3.x d'Apache :
  http://httpd.apache.org/security/vulnerabilities_13.html
- Bulletin de sécurité Freebsd du 1 janvier 2006 :
  http://www.vuxml.org/freebsd/
- Bulletin de sécurité Mandriva MDSKA-2006:007 du 05 janvier 2006 :
  http://wwwnew.mandriva.com/security/advisories?name=MDSKA-2006:007
- Bulletin de sécurité de Red Hat numéro RHA-2006-0158 :
  http://rhn.redhat.com/errata/RHSA-2006-0158.html
- Bulletin de sécurité SUSE SUSE-SR:2006:004 du 24 février 2006 :
  http://www.novell.com/linux/security/advisories/2006_04_sr.html
- Référence CVE CAN-2005-3352 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3352
- Bulletin de mise à jour pour IBM HTTP Server du 13 juin 2006 :
  http://www-1.ibm.com/support/docview.wss?uid=swg24012511

Gestion détaillée du document

15 décembre 2005 version initiale ;
3 janvier 2006 ajout de la référence au bulletin de sécurité FreeBSD ;
10 janvier 2006 ajout de la référence au bulletin de sécurité Mandriva.
27 février 2006 ajout de la référence au bulletin de sécurité SUSE.
22 juin 2006 ajout de la référence au bulletin de mise à jour IBM.