Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 septembre 2006
N° CERTA-2006-AVI-315-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Apache httpd

Gestion du document

Référence	CERTA-2006-AVI-315-003
Titre	Vulnérabilité dans Apache httpd
Date de la première version	01 août 2006
Date de la dernière version	08 septembre 2006
Source(s)	Bulletin de sécurité de l'US-CERT #395412 du 27 juillet 2006
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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

- `Apache httpd` version 1.3.36 et antérieures ;
- `Apache httpd` version 2.0.58 et antérieures ;
- `Apache httpd` version 2.2.2 et antérieures.

3 Résumé

Une vulnérabilité dans le serveur web `Apache httpd` permet à un utilisateur distant mal intentionné de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

`Apache httpd` dispose d'un module nommé *Rewrite* (`mod_rewrite`) permettant la ré-écriture « à la volée » d'adresses réticulaires (`URL`). Une erreur dans ce module permet à un utilisateur distant mal intentionné de réaliser une attaque de type débordement de tampon. Il peut ainsi provoquer un déni de service ou exécuter du code arbitraire sur le serveur vulnérable par le biais d'une requête construite de façon particulière.

`NB` : Bien que ce module ne soit pas activé par défaut dans la version standard de `Apache httpd`, il peut en être autrement dans certaines distributions `GNU/Linux` ou dans d'autres systèmes d'exploitation.

5 Solution

Se référer aux bulletins de sécurité des éditeurs pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Listes des changements apportés aux versions 1.3.36, 2.0.58, 2.2.2 :
  http://www.apache.org/dist/httpd/Announcement1.3.html
  http://www.apache.org/dist/httpd/Announcement2.0.html
  http://www.apache.org/dist/httpd/Announcement2.2.html
- Bulletin de sécurité Debian DSA 1131 du 30 juillet 2006 :
  http://www.debian.org/security/dsa-1131
- Bulletin de sécurité Debian DSA 1132 du 30 juillet 2006 :
  http://www.debian.org/security/dsa-1132
- Bulletin de sécurité Gentoo GLSA 200608-01 du 01 août 2006 :
  http://www.gentoo.org/security/en/glsa/glsa-200608-01.xml
- Bulletin de sécurité SuSE SUSE-SA:2006:043 du 28 juillet 2006 :
  http://www.novell.com/linux/security/advisories/2006_43_apache.html
- Bulletin de sécurité Mandriva MDKSA-2006:133 du 28 juillet 2006 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2006:133
- Bulletin de sécurité Ubuntu USN-328-1 du 27 juillet 2006 :
  http://www.ubuntu.com/usn/usn-328-1
- Correctif de sécurité OpenBSD pour httpd du 31 juillet 2006 :
  http://openbsd.org/errata.html#httpd
- Alerte de sécurité de l'US-CERT #395412 du 27 juillet 2006 :
  http://www.kb.cert.org/vulns/id/395412
- Référence CVE CVE-2006-3747 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3747
- Bulletin de sécurité IBM PK29154 du 14 août 2006 pour IBM HTTP Server 6.x :
  http://www-1.ibm.com/support/docview.wss?uid=swg1PK29154
- Bulletin de sécurité IBM PK29156 du 14 août 2006 pour IBM HTTP Server 2.0.x : 2
  http://www-1.ibm.com/sup port/docview.wss?uid=swg1PK29156
- Bulletin de mise à jour Debian DSA-1167-1 du 04 septembre 2006 :
  http://www.debian.org/security/2006/dsa-1167

Gestion détaillée du document

01 août 2006 version initiale.
04 août 2006 ajout des références aux bulletins de sécurité Gentoo, SuSE, Mandriva et Ubuntu.
21 août 2006 ajout des références IBM HTTP Server PK29154 et PK29156.
08 septembre 2006 ajout de la référence à la mise à jour Debian.