Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 juin 2004
N° CERTA-2004-AVI-167-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités du serveur HTTP Apache

Gestion du document

Référence	CERTA-2004-AVI-167-002
Titre	Multiples vulnérabilités du serveur HTTP Apache
Date de la première version	18 mai 2004
Date de la dernière version	30 juin 2004
Source(s)	Bulletin de sécurité Mandrake MDKSA-2004:046
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

- Déni de service ;
- atteinte à la confidentialité des données ;

2 Systèmes affectés

- Versions du serveur HTTP Apache antérieures à la version 1.3.30 ;
- versions du serveur HTTP Apache antérieures à la version 1.3.31 pour la vulnérabilité sur mod_digest.

3 Description

Deux vulnérabilités sont présentes dans le serveur HTTP Apache :

- Le serveur HTTP Apache ne filtre pas les séquences d'échappement de terminaux dans ses journaux d'erreurs. Cette vulnérabilité peut être exploitée afin de modifier certains fichiers ou bien d'effectuer un déni de service. Cette vulnérabilité est également présente sur Apache 2 sous MacOS X (cf avis CERTA-2004-AVI-156, section documentation) ;
- une vulnérabilité sur le module `mod_digest` (authentification md5) est présente dans la vérification de la réponse d'authentification. Cette vulnérabilité permet à un utilisateur mal intentionné de rejouer une réponse afin de s'authentifier sur le système vulnérable.

4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Avis de sécurité Mandrake MDKSA-2004:046 :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:046
- Avis de sécurité CERTA-2004-AVI-156 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-156/
- Avis de sécurité Gentoo GLSA 200405-22 :
  http://security.gentoo.org/glsa/glsa-200405-22.xml
- Mise à jour de sécurité du paquetage NetBSD apache :
  ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/www/apache/README.html
- Référence CVE pour la première vulnérabilité :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0020
- Référence CVE pour la seconde vulnérabilité :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0987

Gestion détaillée du document

18 mai 2004 version initiale.
27 mai 2004 ajout de la référence au bulletin de sécurité Gentoo.
30 juin 2004 ajout de la référence au bulletin de sécurité NetBSD.