Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 août 2010
N° CERTA-2010-AVI-264-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Apache

Gestion du document

Référence	CERTA-2010-AVI-264-002
Titre	Multiples vulnérabilités dans Apache
Date de la première version	14 juin 2010
Date de la dernière version	02 août 2010
Source(s)	Bulletin de sécurité Apache du 11 juin 2010, mis à jour le 25 juillet 2010
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

- Contournement de la politique de sécurité ;
- atteinte à la confidentialité des données ;
- déni de service à distance.

2 Systèmes affectés

Apache versions 2.2.0, 2.2.2 à 2.2.6, 2.2.8, 2.2.9 à 2.2.15, 2.3.4-alpha, et 2.3.5-alpha.

3 Résumé

De multiples vulnérabilités ont été découvertes dans `Apache`. Elles permettent à une personne malveillante de porter atteinte à la confidentialité des données ou d'effectuer un déni de service à distance.

4 Description

La première vulnérabilité se situe dans le module `mod_proxy_http` d'`Apache`. Elle résulte d'une erreur dans la gestion des *timeout* et permet d'envoyer une réponse à un utilisateur qui ne devrait normalement pas la re-

cevoir. La deuxième vulnérabilité se situe dans les modules `mod_cache` et `mod_dav`. Une personne malveillante peut provoquer un déni de service à distance par le biais d'une requête spécialement conçue.

5 Solution

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

6 Documentation

- Bulletin de sécurité IBM SE44398 du 30 juillet 2010 :
  http://www-01.ibm.com/support/docview.wss?uid=nas2f3abe5f92565651d86257770003c7447
- Référence CVE CVE-2010-2068 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2068
- Référence CVE CVE-2010-1452 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1452

Gestion détaillée du document

14 juin 2010 version initiale.
30 juillet 2010 ajout des informations concernant la vulnérabilité du déni de service et du CVE associé.
02 août 2010 ajout de la référence au bulletin de sécurité IBM.