Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 novembre 2010
N° CERTA-2010-AVI-510-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Apache

Dernière version de ce document : http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-510

Gestion du document

Référence	CERTA-2010-AVI-510-001
Titre	Vulnérabilités dans Apache
Date de la première version	21 octobre 2010
Date de la dernière version	29 novembre 2010
Source(s)	Bulletin de version Apache 2.2 du 19 octobre 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

Déni de service à distance.

2 Systèmes affectés

Apache 2.2.

3 Résumé

Plusieurs vulnérabilités dans Apache permettent à un utilisateur malveillant de provoquer un déni de service à distance.

4 Description

Trois vulnérabilités présentes dans Apache sont exploitables pour provoquer un déni de service à distance :

– CVE-2009-3560 un problème dans la bibliothèque Expat permet de provoquer un arrêt inopiné lors de la lecture d'un fichier XML spécialement conçu ;

– CVE-2009-3720 un autre problème dans la bibliothèque Expat permet de provoquer un arrêt inopiné lors de la lecture d'un fichier XML spécialement conçu ;
– CVE-2010-1623 la fonction *apr_brigade_split_line* peut servir à un utilisateur malveillant pour épuiser la mémoire du serveur.

5 Solution

La version 2.2.17 d'Apache corrige ces problèmes.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

– Bulletin de version Apache 2.2 du 19 octobre 2010 :
http://www.apache.org/dist/httpd/Announcement2.2.html
– Bulletins de sécurité Fedora FEDORA-2010-15916 et 15953 du 28 octobre 2010 :
http://lists.fedoraproject.org/pipermail/package-announce/2010-October/049885.html
http://lists.fedoraproject.org/pipermail/package-announce/2010-October/049939.html
– Bulletin de sécurité Mandriva MDVSA-2010:192 du 02 octobre 2010 :
http://www.mandriva.com/security/advisories?name=MDVSA-2010:192
– Bulletin de sécurité Sun du 26 novembre 2010 :
http://blogs.sun.com/security/entry/cve_2010_1623_memory_leak
– Référence CVE CVE-2009-3560 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3560
– Référence CVE CVE-2009-3720 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3720
– Référence CVE CVE-2010-1623 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1623

Gestion détaillée du document

21 octobre 2010 version initiale.
29 novembre 2010 ajout des bulletins de sécurité Fedora, Mandriva et Sun.