



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 janvier 2003
N° CERTA-2003-AVI-013

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sur le serveur http 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-2003-AVI-013>

Gestion du document

Référence	CERTA-2003-AVI-013
Titre	Vulnérabilité sur le serveur http Apache
Date de la première version	24 janvier 2003
Date de la dernière version	–
Source(s)	Liste de diffusion Bugtraq
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 ;
- exécution de code arbitraire ;
- accès non-autorisé à des fichiers du système.

2 Systèmes affectés

Apache versions antérieures à la version 2.0.44 sur les plates-formes Windows.

3 Résumé

Trois vulnérabilités ont été découvertes sur le serveur http Apache installé sur les plates-formes Windows.

4 Description

Un utilisateur distant mal intentionné peut, par le biais de requête contenant le nom d'un périphérique MS-DOS, réaliser un déni de service de la plate-forme sur laquelle se trouve le serveur http Apache.

Une seconde vulnérabilité permet, dans les mêmes conditions, d'exécuter du code arbitraire sur la machine cible.

Ces deux vulnérabilités ne sont exploitables que sur les plates-formes windows 98 ou windows ME.

La troisième vulnérabilité porte sur la non vérification de caractères spécifiques dans une requête qui permet à un utilisateur mal intentionné, par le biais de requêtes malicieusement construites, d'accéder à des fichiers non autorisés.

5 Solution

La version 2.0.44 corrige ces vulnérabilités.

6 Documentation

Avis sur le site Apache :

<http://httpd.apache.org/dist/httpd/Announcement2.html>

Gestion détaillée du document

24 janvier 2003 version initiale.