Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 octobre 2002
N° CERTA-2002-AVI-224-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités des serveurs HTTP Apache et Oracle

Gestion du document

Référence	CERTA-2002-AVI-224-001
Titre	Vulnérabilités des serveurs HTTP Apache et Oracle
Date de la première version	11 octobre 2002
Date de la dernière version	15 octobre 2002
Source(s)	Avis de sécurité Apache Avis de sécurité Oracle
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 ;
- *cross site scripting* ;
- élévation de privilèges.

2 Systèmes affectés

Serveur HTTP Apache versions 1.3.x antérieures à la version 1.3.26 incluse.
Serveur HTTP Oracle (OHS) présent dans les produits suivants :
- Oracle Database versions 8.1.7, 9.0.1.x et 9.2.x ;
- Oracle9i Application Server versions 1.0.2.x et 9.0.2.x.

3 Résumé

Trois vulnérabilités des serveurs HTTP Apache et Oracle peuvent être exploitées pour provoquer un déni de service, injecter des scripts malicieux, ou réaliser une élévation de privilèges.

4 Description

La première vulnérabilité concerne la table de mémoire partagée. Un utilisateur ayant les privilèges de l'utilisateur *apache* peut exploiter cette vulnérabilité localement pour provoquer un déni de service.

La deuxième vulnérabilité est une vulnérabilité de type *cross site scripting*. Elle peut être exploitée à travers la page d'erreur 404 par défaut, sur tout sytème dans un domaine qui autorise les résolutions DNS avec des métacaractères.

La troisième vulnérabilité, de type débordement de mémoire, concerne le fichier *ab.c*. Cette vulnérabilité peut être exploitée à distance par un utilisateur mal intentionné afin de réaliser une élévation de privilèges.

5 Solution

La version 1.3.27 du serveur Apache corrige ces vulnérabilités.

Nota : les versions 1.2 du serveur Apache ne sont plus maintenues.
Les versions 1.3 ont été conçues pour les systèmes Unix. Dans le cas d'une autre plate-forme, il est fortement recommandé d'installer les versions 2.0.

Des correctifs sont disponibles pour le serveur HTTP Oracle (cf. Section Documentation).

6 Documentation

Avis de sécurité Apache :
http://www.apache.org/dist/httpd/Announcement.html

Correctifs Oracle :
http://metalink.oracle.com

Note d'information CERTA-2002-INF-001 du CERTA sur le Cross Site Scripting :
http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-001/index.html

Gestion détaillée du document

11 octobre 2002 version initiale.
15 octobre 2002 première révision : ajout du serveur HTTP Oracle.