



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 janvier 2005
N° CERTA-2004-AVI-343-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du module `mod_ssl` du 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-2004-AVI-343>

Gestion du document

Référence	CERTA-2004-AVI-343-001
Titre	Vulnérabilité du module <code>mod_ssl</code> du serveur HTTP Apache
Date de la première version	14 octobre 2004
Date de la dernière version	20 janvier 2005
Source(s)	Bulletin de sécurité Apache du 11 octobre 2004
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.

2 Systèmes affectés

Module `mod_ssl` du serveur HTTP Apache versions 2.0.35 à 2.0.52 incluses.

3 Résumé

Une vulnérabilité du module `mod_ssl` du serveur HTTP Apache permet à un utilisateur mal intentionné de contourner la politique de sécurité.

4 Description

Une vulnérabilité a été découverte dans la gestion des paramètres des sessions SSL.

Cette vulnérabilité permet à un utilisateur mal intentionné de contourner la politique de sécurité en se connectant au serveur avec des paramètres uniquement autorisés pour la connexion à l'un des serveurs virtuels.

Pour pouvoir exploiter cette vulnérabilité, le serveur doit être configuré avec la directive `SSLCipherSuite`.

5 Solution

Appliquer les correctifs fournis par l'éditeur (cf. section Documentation).

La version 2.0.53-dev corrige cette vulnérabilité.

6 Documentation

- Site Internet du serveur HTTP Apache :
<http://httpd.apache.org>
- Bulletin de sécurité d'Apache du 11 octobre 2004 :
<http://www.apacheweek.com/features/security-20>
- Correctifs fournis par Apache :
http://nagoya.apache.org/bugzilla/show_bug_cg?id=31505
- Référence CVE CAN-2004-0885 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0885>
- Mise à jour de sécurité pour "VMware ESX Server 2.1.2" :
<http://www.vmware.com/download/esx/esx212-10921update.html>
- Mise à jour de sécurité pour "VMware ESX Server 2.0.1" :
<http://www.vmware.com/download/esx/esx201-11429update.html>
- Mise à jour de sécurité pour "VMware ESX Server 1.5.2" :
<http://www.vmware.com/download/esx/esx152-10816update.html>

Gestion détaillée du document

14 octobre 2004 version initiale.

20 janvier 2005 ajout référence aux mises à jour de sécurité VMware.