



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 septembre 2004
N° CERTA-2004-AVI-195-005

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du module `mod_proxy` 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-195>

Gestion du document

Référence	CERTA-2004-AVI-195-005
Titre	Vulnérabilité du module <code>mod_proxy</code> du serveur HTTP Apache
Date de la première version	11 juin 2004
Date de la dernière version	01 septembre 2004
Source(s)	Avis de sécurité de Georgi Guninski #69 du 10 juin 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

- Déni de service ;
- exécution de code arbitraire.

2 Systèmes affectés

Serveur HTTP Apache versions 1.3.31, 1.3.29, 1.3.28, 1.3.27 et 1.3.26.

3 Résumé

Une vulnérabilité du module `mod_proxy` permet à un utilisateur mal intentionné de provoquer un déni de service sur le serveur vulnérable.

4 Description

Une vulnérabilité de type débordement de mémoire a été découverte dans le module `mod_proxy` du serveur HTTP Apache.

Cette vulnérabilité peut être exploitée à l'aide d'un en-tête *Content-Length* malicieusement choisi. Il faudra pour cela qu'un utilisateur mal intentionné puisse utiliser un serveur Apache vulnérable comme serveur mandataire (*proxy*) pour se connecter à un site web malveillant.

Cela provoquera l'arrêt du processus fils Apache chargé de traiter la requête.

5 Contournement provisoire

Désactiver le module *mod_proxy*.

6 Solution

La version 1.3.32-dev du serveur HTTP Apache corrige cette vulnérabilité.

7 Documentation

- Avis de sécurité de Georgi Guninski #69 du 10 juin 2004 :
<http://www.guninski.com/modproxy1.html>
- Article sur la vulnérabilité *mod_proxy* sur le site d'Apache :
<http://www.apacheweek.com/features/security-13>
- Bulletin de sécurité Debian DSA-525 du 24 juin 2004 :
<http://www.debian.org/security/2004/dsa-525>
- Bulletin de sécurité Gentoo GLSA 200406-16 du 21 juin 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200406-16.xml>
- Bulletin de sécurité Mandrake MDKSA-2004:065 du 29 juin 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:065>
- Bulletin de sécurité RedHat RHSA-2004:245 du 14 juin 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-245.html>
- Bulletin de sécurité OpenBSD pour Apache du 12 juin 2004 :
<http://www.openbsd.org/errata.html>
- Bulletin de sécurité SUN #57628 du 24 août 2004 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-57628-1>
- Référence CVE CAN-2004-0492 :
<http://cve.mitre.org/cgi-bin/cvname.cgi?name=CAN-2004-0492>

Gestion détaillée du document

11 juin 2004 version initiale.

22 juin 2004 ajout des références aux bulletins de sécurité de Gentoo et OpenBSD.

28 juin 2004 ajout de la référence au bulletin de sécurité Debian.

30 juin 2004 ajout de la référence au bulletin de sécurité Mandrake.

06 juillet 2004 ajout de la référence au bulletin de sécurité RedHat.

01 septembre 2004 ajout de la référence au bulletin de sécurité SUN.