



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 septembre 2004
N° CERTA-2004-AVI-106-006

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de tcpdump

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-106>

Gestion du document

Référence	CERTA-2004-AVI-106-006
Titre	Vulnérabilités de tcpdump
Date de la première version	31 mars 2004
Date de la dernière version	08 septembre 2004
Source(s)	Bulletin de sécurité R7-0017 de Rapid7
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.

2 Systèmes affectés

tcpdump versions 3.8.1 et antérieures.

3 Résumé

Deux failles dans l'affichage des paquets ISAKMP (Internet Security Association and Key Management Protocol) ont été identifiées.

4 Description

A l'aide de paquets ISAKMP habilement constitués, un utilisateur mal intentionné peut provoquer un déni de service (arrêt brutal) de l'application tcpdump si celle-ci est employée avec l'option `-v` (visualisation des protocoles).

5 Solution

La version 3.8.3 de tcpdump corrige cette vulnérabilité. Installer cette version à partir des sources ou appliquer le correctif fournit par l'éditeur :

- Sources de tcpdump :
<http://tcpdump.org>

6 Documentation

- Annonce de la sortie de tcpdump 3.8.3 :
<http://tcpdump.org/tcpdump-changes.txt>
- Bulletin de sécurité R7-0017 de Rapid7 :
<http://www.rapid7.com/advisories/R7-0017.html>
- Bulletin de sécurité Debian DSA 478 du 06 avril 2004 :
<http://www.debian.org/security/2004/dsa-478>
- Bulletin de sécurité Gentoo GLSA 200404-03 du 31 mars 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200404-03.xml>
- Bulletin de sécurité Mandrake MDKSA-2004:030 du 14 avril 2004 :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:030>
- Bulletin de sécurité RedHat RHSA-2004:219 du 26 mai 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-219.html>
- Bulletin de sécurité FreeBSD du 31 mars 2004 :
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité Apple du 07 septembre 2004 :
<http://docs.info.apple.com/article.html?artnum=61798>
- Référence CVE CAN-2004-0183 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0183>
- Référence CVE CAN-2004-0184 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0184>

Gestion détaillée du document

31 mars 2004 version initiale.

07 avril 2004 ajout du bulletin de sécurité Debian.

07 avril 2004 ajout du bulletin de sécurité Gentoo.

15 avril 2004 ajout du bulletin de sécurité Mandrake.

12 mai 2004 ajout de la référence au bulletin de sécurité FreeBSD.

09 juin 2004 ajout de la référence au bulletin de sécurité RedHat.

08 septembre 2004 ajout de la référence au bulletin de sécurité Apple.