Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 octobre 2005
N° CERTA-2005-AVI-164-006

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans tcpdump

Gestion du document

Référence	CERTA-2005-AVI-164-006
Titre	Multiples vulnérabilités dans tcpdump
Date de la première version	17 mai 2005
Date de la dernière version	10 octobre 2005
Source(s)	Bulletin de sécurité Mandriva MDKSA-2005:087 Bulletin de sécurité RedHat RHSA-2005:417-05 Bulletin de sécurité RedHat RHSA-2005:421-04
Pièce(s) jointe(s)	

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 3.x.

3 Description

L'application tcpdump est un analyseur réseau.

De nombreuses vulnérabilités découvertes dans différentes fonctions permettent à un utilisateur distant mal intentionné d'effectuer un déni de service en consommant toutes les ressources CPU. L'individu mal intentionné peut exploiter ces vulnérabilités au moyen de paquets GRE, BGP, LDP ou RSVP malicieusement construits.

4 Solution

Se référer au bulletin de sécurité des éditeurs pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Site Internet de l'éditeur :
  http://www.tcpdump.org
- Bulletin de sécurité Mandriva MDKSA-2005:087 du 11 mai 2005 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2005:087
- Bulletin de sécurité Mandriva MDKSA-2005:101 du 15 juin 2005 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2005:101
- Bulletin de sécurité RedHat RHSA-2005:417 du 11 mai 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-417.html
- Bulletin de sécurité RedHat RHSA-2005:421 du 11 mai 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-421.html
- Bulletin de sécurité RedHat RHSA-2005:505 du 13 juin 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-505.html
- Mise à jour de sécurité Fedora Core 2 pour tcpdump du 03 mai 2005 :
  http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/
- Mise à jour de sécurité Fedora Core 3 pour tcpdump du 03 mai 2005 :
  http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/
- Bulletin de sécurité FreeBSD FreeBSD-SA-05:10 du 09 juin 2005 :
  ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:10.tcpdump.asc
- Bulletin de sécurité Gentoo GLSA 200505-06 / tcpdump du 09 mai 2005 (mis à jour le 12 juin 2005) :
  http://www.gentoo.org/security/en/glsa/glsa-200505-06.xml
- Bulletin de sécurité Avaya ASA-2005-137 du 14 juin 2005 :
  http://support.avaya.com/elmodocs2/security/ASA-2005-137_RHSA-2005-417_RHSA-2005-421.pdf
- Bulletin de sécurité SUSE SUSE-SR:2005:017 du 13 juillet 2005 :
  http://www.novell.com/linux/security/advisories/2005_17_sr.html
- Bulletin de sécurité Debian DSA-850 du 09 octobre 2005 :
  http://www.debian.org/security/2005/dsa-850
- Bulletin de sécurité Debian DSA-854 du 09 octobre 2005 :
  http://www.debian.org/security/2005/dsa-854
- Référence CVE CAN-2005-1267 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1267
- Référence CVE CAN-2005-1278 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1278
- Référence CVE CAN-2005-1279 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1279
- Référence CVE CAN-2005-1280 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1280

Gestion détaillée du document

17 mai 2005 version initiale.

10 juin 2005 ajout de la référence au bulletin de sécurité FreeBSD.

14 juin 2005 ajout des références aux bulletins de sécurité Gentoo et RedHat RHSA-2005:505. Ajout de la référence CVE CAN-2005-1267. Modification de la référence au bulletin de sécurité Mandriva.

17 juin 2005 ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:101. Correction des références CVE. Ajout du bulletin de sécurité Avaya ASA-2005-137.

13 juillet 2005 ajout de la référence au bulletin de sécurité SUSE.

10 octobre 2005 ajout des références aux bulletins de sécurité Debian DSA-850 et DSA-854.