

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans 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-2003-AVI-044>

Gestion du document

Référence	CERTA-2003-AVI-044-002
Titre	Multiples vulnérabilités dans tcpdump
Date de la première version	13 mars 2003
Date de la dernière version	25 mars 2003
Source(s)	-
Pièce(s) jointe(s)	Aucune

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Déni de service ;
- Risque de compromission avec les droits de l'utilisateur (généralement *root*).

2 Systèmes affectés

Distributions Linux suivantes :

- Mandrake ;
- Debian ;
- SuSE ;
- Red Hat ;
- Gentoo ;
- Trustix ;
- OpenPKG ;
- Turbolinux.

3 Résumé

Diverses failles concernant l'interprétation de certains protocoles par *tcpdump* ont été identifiées.

4 Description

Des paquets correspondants aux protocoles BGP (« Border Gateway Protocol »), ISAKMP (« Internet Security Association and Key Management Protocol ») ou RADIUS (authentification), spécifiquement falsifiés, peuvent bloquer *tcpdump* et empêcher son utilisateur de voir le trafic réseau.

Par ailleurs, un débordement de mémoire dans la gestion du protocole NFS (« Network File System ») serait exploitable pour s'emparer de l'hôte exécutant *tcpdump*.

5 Solution

Mettre à jour en suivant les recommandations de l'éditeur :

- Mandrake
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:027>
- Debian
<http://www.debian.org/security/2003/dsa-261>
- SuSE
http://www.suse.com/de/security/2003_015_tcpdump.html
- RedHat
<http://rhn.redhat.com/errata/RHSA-2003-085.html>
- Gentoo
<http://forums.gentoo.org/viewtopic.php?t=39378>
- Trustix
<http://www.trustix.net/errata/misc/2003/TSL-2003-0012-tcpdump.asc.txt>
- OpenPKG
<http://www.openpkg.org/security/OpenPKG-SA-2003.014-tcpdump.html>
- Turbolinux
<http://www.turbolinux.com/security/TLSA-2003-14.txt>

6 Documentation

- Avis 02.27.03 d'iDEFENSE :
<http://www.idefense.com/application/poi/display?id=19>
- Références CVE liées au décodage du protocole RADIUS CAN-2003-0093 et CAN-2003-0145 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0093>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0145>
- Référence CVE sur les paquets ISAKMP CAN-2003-0108 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0108>

Gestion détaillée du document

13 mars 2003 version initiale.

14 mars 2003 ajout du bulletin de sécurité SuSE.

25 mars 2003 Ajout des références CVE et des distributions Red Hat, Trustix, OpenPKG et Turbolinux.