

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-2002-AVI-104>

Gestion du document

Référence	CERTA-2002-AVI-104-001
Titre	Vulnérabilités de tcpdump
Date de la première version	17 mai 2002
Date de la dernière version	31 mai 2002
Source(s)	Avis de sécurité Mandrake MDKSA-2002:032
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

Tcpdump versions 3.6.2 et antérieures.

3 Résumé

L'outil *tcpdump* présente des vulnérabilités de type débordement de mémoire permettant un déni de service ou l'exécution de code arbitraire.

4 Description

Tcpdump est un analyseur de trafic réseau.

Plusieurs vulnérabilités de type débordement de mémoire ont été découvertes dans les versions de *tcpdump* antérieures à la version 3.5. D'autres vulnérabilités similaires ont été découvertes dans des versions plus récentes, incluant la version 3.6.2.

Toutes ces vulnérabilités peuvent être exploitées à distance par un utilisateur mal intentionné pour provoquer l'arrêt du processus *tcpdump*, voire exécuter du code arbitraire. Ce code sera exécuté avec les droits de l'utilisateur qui a lancé *tcpdump*. Par défaut, seul l'administrateur *root* y est autorisé.

5 Solution

Consulter les bulletins de sécurité de votre éditeur pour connaître la disponibilité des correctifs.

6 Documentation

- Avis de sécurité Mandrake MDKSA-2002:032 :
<http://www.linux-mandrake.com/en/security/2002/MDKSA-2002-032.php?dis=8.0>
- Avis de sécurité RedHat RHSA-2002:094-08 :
<http://rhn.redhat.com/errata/RHSA-2002-094.html>

Gestion détaillée du document

17 mai 2002 version initiale.

31 mai 2002 première révision : ajout de l'avis Red Hat.