Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 mai 2004
N° CERTA-2004-AVI-008-005

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Failles dans l'analyseur réseau tcpdump

Gestion du document

Référence	CERTA-2004-AVI-008-005
Titre	Failles dans l'analyseur réseau tcpdump
Date de la première version	15 janvier 2004
Date de la dernière version	12 mai 2004
Source(s)	–
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 ;
- risque de compromission avec les droits de l'utilisateur (généralement root).

2 Systèmes affectés

Tout système Unix utilisant *tcpdump*.

3 Résumé

Trois failles ont été identifiées dans le code d'analyse de certains protocoles réseaux. Celles-ci permettent à un utilisateur mal intentionné distant de bloquer ou d'arrêter inopinément le programme, voire d'exécuter du code arbitraire.

4 Description

Deux des vulnérabilités concernent l'analyse des paquets ISAKMP (port 500) et conduisent soit à une boucle infinie, soit à une erreur d'accès mémoire (références CVE CAN-2003-0989 et CAN-2004-0057). Une mauvaise

validation de la taille des champs d'un paquet RADIUS (port 1812) peut produire le même type d'erreur (référence CVE CAN-2004-0055).

5 Solution

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

- Avis de sécurité Red Hat Linux RHSA-2004:007-10 :
  https://rhn.redhat.com/errata/RHSA-2004-007.html
- Avis de sécurité SuSE Linux SuSE-SA:2004:002 :
  http://www.suse.com/de/security/2004_02_tcpdump.html
- Avis de sécurité Debian DSA-425-1 :
  http://www.debian.org/security/2004/dsa-425
- Avis de sécurité Mandrake MDKSA-2004:008 :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:008
- Avis de sécurité Fedora FEDORA-2004-091 :
  http://www.redhat.com/archives/fedora-announce-list/2004-March/msg00009.html
- Avis de sécurité FreeBSD du 19 janvier 2004 :
  http://www.vuxml.org/freebsd/

6 Documentation

- Référence CVE CAN-2003-0989 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0989
- Référence CVE CAN-2004-0055 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0055
- Référence CVE CAN-2004-0057 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0057

Gestion détaillée du document

15 janvier 2004 version initiale ;
19 janvier 2004 ajout de la référence au bulletin de sécurité de Debian.
27 janvier 2004 ajout de la référence au bulletin de sécurité de Mandrake.
03 mars 2004 ajout de la référence au bulletin de sécurité de Fedora FEDORA-2004-090.
05 mars 2004 modification de la référence au bulletin de sécurité de Fedora FEDORA-2004-091.
12 mai 2004 ajout référence au bulletin de sécurité FreeBSD.