

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Tcpcdump

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-2007-AVI-323>

Gestion du document

Référence	CERTA-2007-AVI-323-002
Titre	Vulnérabilité dans Tcpcdump
Date de la première version	19 juillet 2007
Date de la dernière version	01 août 2007
Source(s)	Bulletin de sécurité Secunia SA26135 du 19 juillet 2007
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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

- Tcpcdump, pour la version 3.9.6 ainsi que celles antérieures.

3 Résumé

Une vulnérabilité a été identifiée dans l'outil d'analyse de trafic réseau `tcpcdump`. L'exploitation de cette dernière pourrait permettre l'exécution de code arbitraire sur le système utilisant une version vulnérable.

4 Description

Une vulnérabilité a été identifiée dans l'outil d'analyse de trafic réseau `tcpcdump`. Il ne manipulerait pas correctement certains paquets du protocole BGP (Border Gateway Protocol), utilisé pour des échanges d'information

sur le routage. Cette vulnérabilité, de type « débordement de tampon », peut être exploitée par un utilisateur distant envoyant un paquet spécialement construit. Cette exploitation permettrait l'exécution de code arbitraire sur le système utilisant une version vulnérable.

5 Solution

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

Il n'y a pas de mise à jour officielle de `tcpdump` à la date de rédaction de cet avis. Cependant, un *patch* est disponible dans le répertoire SVN du projet.

6 Documentation

- Référence CVE CVE-2007-3798 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3798>
- Bulletin de sécurité Gentoo GLSA-200707-14 du 28 juillet 2007 :
<http://www.gentoo.org/en/glsa/glsa-200707-14.xml>
- Bulletin de sécurité Mandriva MDKSA-2007:148 du 25 juillet 2007 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:148>
- Bulletin de sécurité Ubuntu USN-492-1 du 30 juillet 2007 :
<http://www.ubuntu.com/usn/usn-492-1>
- Avis de sécurité Secunia SA26135 du 19 juillet 2007 :
<http://secunia.com/advisories/26135/>
- Correctif disponible sous forme de patch dans le répertoire CVS :
<http://cvs.tcpdump.org/cgi-bin/cvsweb/tcpdump/print-bgp.c?r1=1.91.2.11&r2=1.91.2.12>

Gestion détaillée du document

19 juillet 2007 version initiale.

27 juillet 2007 ajout de la référence au bulletin de sécurité Mandriva.

01 août 2007 ajout des références aux bulletins de sécurité Gentoo et Ubuntu.