

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité 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-268>

---

### Gestion du document

Référence	CERTA-2002-AVI-268
Titre	Vulnérabilité de tcpdump
Date de la première version	13 décembre 2002
Date de la dernière version	–
Source(s)	Avis de sécurité CSSA-2002-050 de Caldera
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

Les versions de tcpdump antérieures à la version 3.6.2-2.2.

## 3 Résumé

Une vulnérabilité présente dans le traitement des paquets BGP (Border Gateway Protocol) permet à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code à distance.

## 4 Description

BGP est un protocole chargé d'établir et de partager les informations de routage.  
L'analyseur de trafic `tcpdump` permet de visualiser le trafic de plusieurs protocoles réseaux.

Une vulnérabilité sur le traitement du protocole BGP dans `tcpdump` permet à un utilisateur mal intentionné d'exécuter du code arbitraire avec les privilèges de l'utilisateur de l'application `tcpdump`.

## **5 Solution**

Appliquer le correctif correspondant à votre plate-forme (cf. section documentation).

## **6 Documentation**

- Avis de sécurité de Linux Debian  
<http://www.debian.org/security/2002/dsa-206>
- Avis de sécurité de Linux Caldera  
<ftp://ftp.sco.com/pub/security/OpenLinux/CSSA-2002-050.0.txt>

## **Gestion détaillée du document**

**13 décembre 2002** version initiale.