

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de l2tpd

---

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-2004-AVI-248>

---

### Gestion du document

Référence	CERTA-2004-AVI-248-001
Titre	Vulnérabilité de l2tpd
Date de la première version	19 juillet 2004
Date de la dernière version	22 juillet 2004
Source(s)	Bulletin de sécurité Debian DSA-530 du 17 juillet 2004
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

- Dénis de service ;
- exécution de code arbitraire à distance.

## 2 Systèmes affectés

Toutes les versions de l2tpd.

## 3 Description

l2tpd est un service pour le protocole L2TP (Layer 2 Tunneling Protocol).  
Un débordement de mémoire dans l2tpd permet à un utilisateur mal intentionné, via l'envoi d'un paquet malicieusement construit, d'exécuter du code arbitraire à distance sur la plate-forme vulnérable.

## 4 Solution

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

## 5 Documentation

- Site Internet de l2tpd :  
<http://www.l2tpd.org>
- Bulletin de sécurité Debian DSA-530 du 17 juillet 2004 :  
<http://www.debian.org/security/2004/dsa-530>
- Bulletin de sécurité Gentoo GLSA 200407-17 du 22 juillet 2004 :  
<http://www.gentoo.org/security/en/glsa/glsa-200407-17.xml>
- Référence CVE CAN-2004-0649 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0649>

### Gestion détaillée du document

**19 juillet 2004** version initiale.

**22 juillet 2004** ajout de la référence au bulletin de sécurité Gentoo.