



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 24 août 2006  
N° CERTA-2006-AVI-370

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans ppp

---

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-2006-AVI-370>

---

### Gestion du document

Référence	CERTA-2006-AVI-370
Titre	Vulnérabilité dans ppp
Date de la première version	24 août 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Ubuntu USN-310-1
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

Élévation de privilèges.

## 2 Systèmes affectés

ppp versions 2.4.3 et antérieures.

## 3 Résumé

Une vulnérabilité dans ppp permet à un utilisateur local d'élever ses privilèges sur le système vulnérable.

## 4 Description

Un manque de contrôle de la valeur de retour de la fonction *setuid()* dans l'extension *winbind* du service *pppd* de *ppp* permet à un utilisateur local d'élever ses privilèges.

## 5 Solution

La version 2.4.4 de `ppp` corrige le problème :  
<ftp://ftp.samba.org/pub/ppp/>

## 6 Documentation

- Bulletin de sécurité Debian DSA 1106 du 10 juillet 2006 :  
<http://www.debian.org/security/dsa-1106>
- Bulletin de sécurité Mandriva MDKSA-2006:119 du 10 juillet 2006 :  
<http://www.mandriva.com/security/advisories?name=MDKSA-2006:119>
- Bulletin de sécurité Ubuntu USN-310-1 du 10 juillet 2006 :  
<http://www.ubuntu.com/usn/usn-310-1>
- Référence CVE CVE-2006-2194 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2194>

## Gestion détaillée du document

**24 août 2006** version initiale.