



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 novembre 2001
N° CERTA-2001-AVI-142

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des utilitaires '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-2001-AVI-142>

Gestion du document

Référence	CERTA-2001-AVI-142
Titre	Vulnérabilité des utilitaires 'ppp'
Date de la première version	16 novembre 2001
Date de la dernière version	–
Source(s)	Avis de sécurité 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

Obtention des droits de l'utilisateur *root*.

2 Systèmes affectés

Utilitaires liés à *pppattach*.

3 Résumé

Un utilisateur mal intentionné peut, en local, obtenir les droits de l'utilisateur *root* en exploitant une vulnérabilité des utilitaires liés à *pppattach*.

4 Description

PPP (Point to Point Protocol) est un protocole utilisé pour échanger des paquets IP sur une liaison série.

Il existe une vulnérabilité des exécutables liés à *pppattach*, permettant à un utilisateur d'obtenir, en local, les droits du propriétaire du fichier */usr/bin/pppattach* (drapeau *setuid* positionné).

Le propriétaire par défaut de ce fichier est l'utilisateur *root*.

5 Contournement provisoire

Si vous n'utilisez pas le protocole PPP, désinstallez les utilitaires PPP, ou désactivez le drapeau *setuid root* du fichier */usr/bin/pppattach*.

6 Solution

Contactez votre distributeur pour obtenir une mise à jour.

7 Documentation

Bulletin de sécurité Caldera :
<http://stage.caldera.com/support/security>

Gestion détaillée du document

16 novembre 2001 version initiale.