Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 mai 2005
N° CERTA-2005-AVI-119-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du noyau Linux

Gestion du document

Référence	CERTA-2005-AVI-119-001
Titre	Vulnérabilité du noyau Linux
Date de la première version	22 mars 2005
Date de la dernière version	23 mai 2005
Source(s)	
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 à distance.

2 Systèmes affectés

Tout système utilisant un noyau Linux.

3 Résumé

Une faille a été identifiée dans le pilote noyau du protocole PPP (« Point to Point Protocol ») qui permet à un client mal intentionné de suspendre le fonctionnement de l'hôte.

4 Description

PPP est utilisé pour réaliser des connexions point à point, en particulier pour établir une communication avec un fournisseur d'accès via une ligne téléphonique que ce soit du RTC ou de l'ADSL.

L'envoi d'un paquet volontairement mal formé à un serveur PPP (souvent appelé pppd) bloque le noyau dans une boucle infinie. Du code malicieux est publiquement disponible.

5 Solution

Mettre à jour les sources du noyau (2.4.30-rc1 ou 2.6.11.4 au moins) ou consulter le bulletin de l'éditeur pour l'obtention d'un correctif (cf. section Documentation).

6 Documentation

- Sources du noyau Linux :
  http://www.kernel.org
- Gentoo Linux, utiliser un noyau postérieur au 2.6.11-r4 :
  http://bugs.gentoo.org/show_bug.cgi?id=82201
- Red Hat Enterprise Linux :
  http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=151240
  http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=151241
  http://rhn.redhat.com/errata/RHSA-2005-283.html
  http://rhn.redhat.com/errata/RHSA-2005-284.html
  http://rhn.redhat.com/errata/RHSA-2005-366.html
- Bulletin de sécurité SUSE SuSE-SA:2005:018 :
  http://www.novell.com/linux/security/advisories/2005_018_kernel.html
- Référence CVE CAN-2005-0384 du 14 février 2005 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0384

Gestion détaillée du document

22 mars 2005 version initiale ;
23 mai 2005 ajout des bulletins de sécurité Red Hat, SuSE et de la référence CVE.