Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 18 juillet 2006
N° CERTA-2006-AVI-295

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de la fonction prctl du noyau Linux

Gestion du document

Référence	CERTA-2006-AVI-295
Titre	Vulnérabilité de la fonction prctl du noyau Linux
Date de la première version	18 juillet 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité RedHat du 07 juillet 2006
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 ;
- contournement de la politique de sécurité ;
- élévation de privilèges.

2 Systèmes affectés

Les noyaux Linux, des versions 2.6.13 jusqu'à la version 2.6.17.4 non comprise, et 2.6.16 antérieure à 2.6.16.24.

3 Description

`prctl` est une fonction du noyau Linux permettant d'effectuer certaines opérations sur les processus. Il est aussi possible, depuis les versions 2.6.13 du noyau Linux, de spécifier si les processus peuvent créer des fichiers `core dump`, et sous quelles conditions. Cela peut être un argument de la fonction `prctl`. Une vulnérabilité a été identifiée dans celle-ci combinée à un tel argument.

Un utilisateur malveillant local peut profiter de cette vulnérabilité pour élever ses privilèges à ceux d'administrateur (`root`) sur le système affecté.

4 Solution

Se référer aux différents bulletins de sécurité pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Mise à jour de sécurité Fedora Core 4 du 15 juillet 2006 :
  http://download.fedora.redhat.com/pub/fedora/linux/core/updates/4/
- Bulletin de sécurité RedHat RHSA-2006:0574 du 07 juillet 2006 :
  http://rhn.redhat.com/errata/RHSA-2006-0574.html
- Bulletin de sécurité Ubuntu USN-311-1 du 11 juillet 2006 :
  http://www.ubuntulinux.org/usn/usn-311-1
- Référence CVE CVE-2006-2451 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2451
- Mise à jour des noyaux Linux :
  http://www.kernel.org/pub/linux/kernel/v2.6/

Gestion détaillée du document

18 juillet 2006 version initiale.