

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité du noyau Linux

---

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-2007-AVI-416>

---

### Gestion du document

Référence	CERTA-2007-AVI-416
Titre	Vulnérabilité du noyau Linux
Date de la première version	24 septembre 2007
Date de la dernière version	–
Source(s)	Liste des changements apportés aux versions 2.4.35.3 et 2.6.22.7 du noyau Linux
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

- Linux kernel versions 2.4.35.2 et antérieures ;
- Linux kernel versions 2.6.22.6 et antérieures.

## 3 Résumé

Une vulnérabilité dans le noyau Linux permet à un utilisateur local d'élever ses privilèges.

## 4 Description

Une vulnérabilité dans la mise en œuvre de l'appel système *ptrace* par le noyau Linux permet à un utilisateur local d'élever ses privilèges. La faille est relative à une mauvaise initialisation de registre sur une architecture *x86\_64* lors de la sortie d'un appel système *ptrace* en mode *32bit*.

## 5 Solution

Les versions 2.4.35.3 et 2.6.22.7 du noyau Linux corrigent le problème :

<http://www.kernel.org/pub/linux/kernel/v2.4/>

<http://www.kernel.org/pub/linux/kernel/v2.6/>

## 6 Documentation

- Site du noyau Linux :  
<http://www.kernel.org>
- Liste des changements apportés à la version 2.4.35.3 du noyau Linux :  
<http://www.kernel.org/pub/linux/kernel/v2.4/Changelog-2.4.35.3>
- Liste des changements apportés à la version 2.6.22.7 du noyau Linux :  
<http://www.kernel.org/pub/linux/kernel/v2.4/Changelog-2.6.22.7>
- Référence CVE CVE-2007-4573 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4573>

## Gestion détaillée du document

**24 septembre 2007** version initiale.