

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans le 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-256>

Gestion du document

Référence	CERTA-2007-AVI-256
Titre	Multiples vulnérabilités dans le noyau Linux
Date de la première version	08 juin 2007
Date de la dernière version	–
Source(s)	Liste des changements apportés à la version 2.6.21.4 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

- Dénis de service à distance ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Noyau Linux 2.6.

3 Résumé

Plusieurs vulnérabilités dans la branche 2.6 du noyau Linux permettent à un utilisateur malintentionné de provoquer un déni de service à distance ou de porter atteinte à la confidentialité des données.

4 Description

- Une vulnérabilité dans NETFILTER permet à une personne malveillante de provoquer un déni de service du système au moyen d'un paquet SCTP (*Stream Control Transmission Protocol* spécialement construit (CVE-2007-2876)) ;

- la seconde vulnérabilité dans la fonction `cpuset_tasks_read` permet à un individu malintentionné d’avoir accès en lecture à la certaine zone mémoire du noyau Linux (CVE-2007-2875) ;
- une faiblesse dans le noyau Linux lors du traitement des graines utilisées pour la création de nombres aléatoires. Cela peut fragiliser toute application s’appuyant sur ce générateur de nombre aléatoire (CVE-2007-2453).

5 Solution

Se référer au bulletin de sécurité de l’éditeur pour l’obtention des correctifs (cf. section Documentation).

6 Documentation

- Liste des changements apportés à la version 2.6.21.4 du noyau Linux :
<http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.21.4>
- Référence CVE CVE-2007-2453 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2453>
- Référence CVE CVE-2007-2875 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2875>
- Référence CVE CVE-2007-2876 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2876>

Gestion détaillée du document

08 juin 2007 version initiale.