Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 juin 2008
N° CERTA-2008-AVI-252-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités du noyau Linux

Gestion du document

Référence	CERTA-2008-AVI-252-001
Titre	Multiples vulnérabilités du noyau Linux
Date de la première version	19 mai 2008
Date de la dernière version	25 juin 2008
Source(s)	Liste des changements apportés dans la version 2.6.25.3 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

- Déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

Les noyaux Linux versions 2.6.25.2 et antérieures.

3 Résumé

Plusieurs vulnérabilités présentes dans le noyau `Linux` permettent à un utilisateur distant de provoquer un déni de service ou à un utilisateur local de contourner la politique de sécurité du système.

4 Description

Plusieurs vulnérabilités sont présentes dans le noyau `Linux` :

- la première est relative à l'appel système *sys_utimensat()*. Elle permet à un utilisateur local de modifier les dates d'accès ou de modifications d'un fichier arbitraire sans tenir compte des droits d'accès normaux ;

– la deuxième concerne le pilote mettant en œuvre l'encapsulation `IPv6` dans `IPv4` et permet à un utilisateur distant de provoquer une consommation excessive de la mémoire via un paquet particulier ;
– la dernière concerne la fonction *mmap()* sur architecture de type `SPARC`. Cette vulnérabilité permet à un utilisateur local de provoquer un déni de service du système vulnérable.

5 Solution

La version 2.6.25.3 du noyau `Linux` corrige le problème :
http://www.kernel.org
Se référer au bulletin de sécurité des éditeurs de distributions pour l'obtention de correctifs (cf. section Documentation).

6 Documentation

– Liste des changements apportés dans la version 2.6.25.3 du noyau `Linux` :
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.25.3
– Bulletin de sécurité OpenSUSE SUSE-SA:2008:030 du 20 juin 2008 :
http://lists.opensuse.org/opensuse-security-announce/2008-06/msg00006.html
– Référence CVE CVE-2008-2136 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2136
– Référence CVE CVE-2008-2137 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2137
– Référence CVE CVE-2008-2148 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2148

Gestion détaillée du document

19 mai 2008 version initiale.
25 juin 2008 ajout de la référence au bulletin de sécurité OpenSUSE.