

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-2008-AVI-297>

Gestion du document

Référence	CERTA-2008-AVI-297
Titre	Vulnérabilité du noyau Linux
Date de la première version	09 juin 2008
Date de la dernière version	–
Source(s)	Liste des changements apportés aux versions 2.4.36.6 et 2.6.25.5 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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

- le noyau Linux versions 2.4.36.5 et antérieures ;
- le noyau Linux versions 2.6.25.4 et antérieures.

3 Résumé

Une vulnérabilité présente dans le noyau Linux permet à un utilisateur distant de provoquer un déni de service ou potentiellement d'exécuter du code arbitraire.

4 Description

Une vulnérabilité est présente dans le noyau Linux. Celle-ci est relative à la mise en œuvre du standard ASN . 1 (Abstract Syntax Notation version 1) par le decodeur BER des modules *cifs* et *ip_nat_nmp_basic*.

Un utilisateur distant malintentionné peut provoquer un déni de service ou potentiellement exécuter du code arbitraire via des données encodées au format BER ASN.1.

5 Solution

Les versions 2.4.36.6 et 2.6.25.5 corrigent le problème :

- <http://www.kernel.org>

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

6 Documentation

- liste des changements apportées aux versions 2.4.36.6 et 2.6.25.5 du noyau Linux :
<http://kernel.org/pub/linux/kernel/v2.4/ChangeLog-2.4.36.6>
<http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.25.5>
- Référence CVE CVE-2008-1673 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1673>

Gestion détaillée du document

09 juin 2008 version initiale.