

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités des noyaux Linux 2.6

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-2004-AVI-356>

Gestion du document

Référence	CERTA-2004-AVI-356
Titre	Vulnérabilités des noyaux Linux 2.6
Date de la première version	22 octobre 2004
Date de la dernière version	–
Source(s)	Avis de sécurité SuSE SA:2004:037 du 20 octobre 2004
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 ;
- exécution de code arbitraire (architecture s390).

2 Systèmes affectés

Toute distribution Linux utilisant un noyau 2.6 non corrigé.

3 Résumé

Deux failles ont été identifiées dans les versions 2.6 du noyau Linux :

- il est possible d'envoyer au système vulnérable un paquet IP volontairement mal formé qui provoquera un déni de service ;
- une faille sur architecture s390 peut être exploitée par un utilisateur mal intentionné pour exécuter du code arbitraire.

4 Description

- Vulnérabilité du système de filtrage IP *netfilter* (référence CVE CAN-2004-0816) : un individu distant mal intentionné peut transmettre un paquet IP habilement construit qui provoquera un déni de service, suite à débordement d'entier, lors de sa journalisation par *netfilter*.
- Vulnérabilité de l'architecture s390 (référence CVE CAN-2004-0887) : la mauvaise gestion d'une instruction privilégiée permet à un utilisateur mal intentionné d'exécuter du code arbitraire.

5 Solution

La version 2.6.8 des sources du noyau corrige la vulnérabilité *netfilter*.

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

6 Documentation

- Bulletin de sécurité SUSE SuSE-SA:2004:037 du 20 octobre 2004 :
http://www.suse.com/de/security/2004_37_kernel.html
- Avis de sécurité Secunia du 21 octobre 2004 concernant le pare-feu Linux :
<http://secunia.com/advisories/11202/>
- Référence CVE CAN-2004-0816 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0816>
- Référence CVE CAN-2004-0887 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0887>

Gestion détaillée du document

22 octobre 2004 version initiale.