

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités 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-2004-AVI-225>

---

### Gestion du document

Référence	CERTA-2004-AVI-225-002
Titre	Multiples vulnérabilités du noyau Linux
Date de la première version	06 juillet 2004
Date de la dernière version	22 juillet 2004
Source(s)	Bulletin de sécurité Gentoo GLSA-200407-02 du 03 juillet 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

- Elévation de privilèges ;
- déni de service ;
- divulgation d'informations confidentielles.

## 2 Systèmes affectés

Noyau Linux versions 2.4.x et 2.6.x.

## 3 Résumé

De multiples vulnérabilités ont été découvertes dans le noyau Linux.

## 4 Description

Plusieurs distributions ont fourni des correctifs pour des vulnérabilités du noyau Linux. Certaines de ces vulnérabilités ont déjà fait l'objet d'avis du CERTA.

- Une vulnérabilité de type débordement de mémoire est présente dans deux fonctions du noyau Linux relatives à la gestion des liens symboliques du système de fichiers ISO9600 (CVE CAN-2004-0109). Cette vulnérabilité a fait l'objet de l'avis CERTA-2004-AVI-131 du 27 avril 2004.
- Une vulnérabilité est présente dans le code du système de fichiers XFS, et provoque une fuite d'informations (CVE CAN-2004-0133). Des vulnérabilités similaires existent pour le système de fichiers ext3 (CVE CAN-2004-0177) et pour le système de fichiers JFS (CVE CAN-2004-0181).
- Une vulnérabilité du code OSS pour le pilote *Sound Blaster* permet à un utilisateur mal intentionné de provoquer un déni de service (CVE CAN-2004-0178).
- Une vulnérabilité dans la gestion des entiers non signés du composant *cpufreq* permet à un utilisateur local d'élever ses privilèges (CVE CAN-2004-0228).
- Une vulnérabilité existe dans la fonction *fb\_copy\_cmap* (CVE CAN-2004-0299).
- Une vulnérabilité de type débordement de mémoire est présente dans la fonction *panic()* des noyaux 2.4.x (CVE CAN-2004-0394).
- Une mauvaise gestion du compteur *mm\_count* par la fonction *do\_fork* permet de provoquer un déni de service (CVE CAN-2004-0427).
- Une vulnérabilité du noyau Linux pour les systèmes *ia64* permet de provoquer un déni de service (CVE CAN-2004-0447).
- Plusieurs vulnérabilités ont été découvertes par l'outil de vérification de code source *Sparse* (CVE CAN-2004-0495).
- D'autres vulnérabilités ont également été découvertes, qui permettent à un utilisateur local d'élever ses privilèges ou d'accéder à l'espace mémoire du noyau (CVE CAN-2004-0496).
- Des vulnérabilités du noyau Linux permettent à un utilisateur local de modifier l'identifiant du groupe de fichiers (CVE CAN-2004-0497).
- Une mauvaise gestion de la mémoire dans le pilote *e1000* permet à un utilisateur de lire certaines portions de l'espace mémoire du noyau (CVE CAN-2004-0535).
- Une vulnérabilité de *x86* permet à un utilisateur local mal intentionné de provoquer un déni de service (CVE CAN-2004-0554).
- Une vulnérabilité est présente pour les systèmes *ia64* (CVE CAN-2004-0565).
- Des permissions non appropriées du fichier */proc/scsi/qla2300/HbaApiNode* permettent à un utilisateur local mal intentionné de provoquer un déni de service (CVE CAN-2004-0587).
- Une vulnérabilité de la fonction *tcp\_find\_option* du sous-système *netfilter* lors de l'utilisation d'*iptables* et des options TCP permet à un utilisateur distant de provoquer un déni de service (CVE CAN-2004-0626). Cette vulnérabilité a fait l'objet de l'avis CERTA-2004-AVI-224 du 06 juillet 2004.

## 5 Solution

Appliquer le correctif proposé par votre éditeur.

- Le correctif Gentoo GLSA 200407-02 corrige les vulnérabilités suivantes :
  - CVE CAN-2004-0109 ;
  - CVE CAN-2004-0133 ;
  - CVE CAN-2004-0177 ;
  - CVE CAN-2004-0178 ;
  - CVE CAN-2004-0181 ;
  - CVE CAN-2004-0228 ;
  - CVE CAN-2004-0229 ;
  - CVE CAN-2004-0394 ;
  - CVE CAN-2004-0427 ;
  - CVE CAN-2004-0495 ;
  - CVE CAN-2004-0535 ;
  - CVE CAN-2004-0554.
- Le correctif Gentoo GLSA 200407-16 corrige les vulnérabilités suivantes :
  - CVE CAN-2004-0447 ;
  - CVE CAN-2004-0496 ;

- CVE CAN-2004-0497 ;
- CVE CAN-2004-0565.
- Les correctifs RedHat corrigent les vulnérabilités suivantes :
  - CVE CAN-2004-0497 (RHSA-2004:354 et RHSA-2004:360) ;
  - CVE CAN-2004-0427, CAN-2004-0495 et CAN-2004-0554 (RHSA-2004:255).
- Le correctif SuSE corrige les vulnérabilités suivantes:
  - CVE CAN-2004-0495 ;
  - CVE CAN-2004-0496 ;
  - CVE CAN-2004-0497 ;
  - CVE CAN-2004-0535 ;
  - CVE CAN-2004-0626.
- Le correctif Mandrake MDKSA-2004:062 corrige les vulnérabilités suivantes :
  - CVE CAN-2004-0535 ;
  - CVE CAN-2004-0554.
- Le correctif Mandrake MDKSA-2004:066 corrige les vulnérabilités suivantes :
  - CVE CAN-2004-0495 ;
  - CVE CAN-2004-0497 ;
  - CVE CAN-2004-0565 ;
  - CVE CAN-2004-0587.

## 6 Documentation

- Site Internet du noyau Linux :  
<http://www.kernel.org>
- Bulletin de sécurité Gentoo GLSA 200407-02 du 03 juillet 2004 :  
<http://www.gentoo.org/security/en/glsa/glsa-200407-02.xml>
- Bulletin de sécurité Gentoo GLSA 200407-16 du 22 juillet 2004 :  
<http://www.gentoo.org/security/en/glsa/glsa-200407-16.xml>
- Bulletin de sécurité Mandrake MDKSA-2004:062 du 23 juin 2004 :  
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:062>
- Bulletin de sécurité Mandrake MDKSA-2004:066 du 06 juillet 2004 :  
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:066>
- Bulletin de sécurité RedHat RHSA-2004:354 du 02 juillet 2004 :  
<http://rhn.redhat.com/errata/RHSA-2004-354.html>
- Bulletin de sécurité RedHat RHSA-2004:360 du 02 juillet 2004 :  
<http://rhn.redhat.com/errata/RHSA-2004-360.html>
- Avis de sécurité CERTA-2004-AVI-131 du 27 avril 2004 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-131/index.html>
- Avis de sécurité CERTA-2004-AVI-224 du 06 juillet 2004 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-224/index.html>

## Gestion détaillée du document

**06 juillet 2004** version initiale.

**07 juillet 2004** ajout des références CVE CAN-2004-0565 et CVE CAN-2004-0587 et ajout de la référence au bulletin de sécurité Mandrake MDKSA-2004:066.

**22 juillet 2004** ajout de la référence au second bulletin de sécurité Gentoo GLSA 200407-16 ainsi que la description de la vulnérabilité CVE CAN-2004-0447.