Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 février 2005
N° CERTA-2005-AVI-023-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités du noyau Linux

Gestion du document

Référence	CERTA-2005-AVI-023-001
Titre	Multiples vulnérabilités du noyau Linux
Date de la première version	24 janvier 2005
Date de la dernière version	21 février 2005
Source(s)	Bulletin de sécurité RedHat RHSA-2005:043-13 du 18 janvier 2005
Pièce(s) jointe(s)	

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Elévéation de privilège ;
- déni de service.

2 Systèmes affectés

- Red Hat Desktop v.3 ;
- Red Hat Enterprise Linux AS v.3 ;
- Red Hat Enterprise Linux ES v.3 ;
- Red Hat Enterprise Linux WS v.3.

3 Résumé

De nombreuses vulnérabilités découvertes dans le noyau Linux permettent à un utilisateur mal intentionné d'augmenter ses privilèges ou d'effectuer un déni de service sur le système vulnérable.

4 Description

- CAN-2004-1235 : Une vulnérabilité affectant l'appel système `uselib(2)` du noyau Linux permet à un utilisateur local mal intentionné d'élever ses privilèges.
- CAN-2004-1237 : Le sous système d'audit dans la distribution Red Hat Enterprise Linux 3 présente une vulnérabilité permettant à une personne malveillante d'effectuer localement un déni de service sur le système.
- CAN-2005-0001 : Une vulnérabilité découverte dans le noyau Linux peut être exploitée localement par un utilisateur mal intentionné dans le but d'élever ses privilèges.
- CAN-2005-0003 : Une dernière vulnérabilité présente dans le noyau Linux permet à une personne malveillante d'effectuer un déni de service sur le système vulnérable, au moyen d'un fichier binaire au format `a.out` ou au format `ELF` malicieusement construit.

5 Solution

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

6 Documentation

- Bulletin de sécurité iSec Security Research du 12 janvier 2005 :
  http://www.isec.pl/vulnerabilities/isec-0022-pagefault.txt
- Bulletin de sécurité iSec Security Research du 07 janvier 2005 :
  http://www.isec.pl/vulnerabilities/isec-0021-uselib.txt
- Bulletin de sécurité RedHat RHSA-2005:043-13 du 18 janvier 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-043.html
- Bulletin de sécurité RedHat RHSA-2005:092-14 du 18 février 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-092.html

Gestion détaillée du document

24 janvier 2005 version initiale.
21 février 2005 ajout de la référence au bulletin de sécurité RedHat RHSA-2005:092-14.