Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 janvier 2005
N° CERTA-2004-AVI-265-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du noyau Linux

Gestion du document

Référence	CERTA-2004-AVI-265-002
Titre	Vulnérabilité du noyau Linux
Date de la première version	05 août 2004
Date de la dernière version	20 janvier 2005
Source(s)	Avis de sécurité d'ISEC du 04 août 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

Divulgation d'informations confidentielles.

2 Systèmes affectés

- Noyau Linux versions 2.4.26 et antérieures ;
- noyau Linux versions 2.6.7 et antérieures.

3 Résumé

Une vulnérabilité du noyau Linux permet à un utilisateur local mal intentionné d'avoir accès à des informations confidentielles.

4 Description

Une vulnérabilité a été découverte dans le traitement des pointeurs vers les indices de décalage dans les fichiers (*file offset)* sur 64 bits.

Un utilisateur local mal intentionné peut exploiter cette vulnérabilité pour accèder à certaines parties de la mémoire du noyau. Il est possible d'y trouver certaines informations confidentielles (mots de passe par exemple).

5 Solution

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

6 Documentation

- Avis de sécurité d'ISEC du 04 août 2004 :
  http://isec.pl/vulnerabilities/isec-0016-procleaks.txt
- Site Internet du noyau Linux :
  http://www.kernel.org
- Bulletin de sécurité RedHat RHSA-2004:413 du 03 août 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-413.html
- Bulletin de sécurité RedHat RHSA-2004:418 du 03 août 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-418.html
- Bulletin de sécurité SuSE SuSE-SA:2004:024 du 09 août 2004 :
  http://www.suse.com/de/security/2004_24_kernel.html
- Bulletin de sécurité Gentoo GLSA 200408-24 du 25 août 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200408-24.xml
- Bulletin de sécurité Mandrake MDKSA-2004:087 du 26 août 2004 :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:087
- Référence CVE CAN-2004-0415 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0415
- Mise à jour de sécurité pour "VMware ESX Server 2.1.2" :
  http://www.vmware.com/download/esx/esx212-10921update.html
- Mise à jour de sécurité pour "VMware ESX Server 2.0.1" :
  http://www.vmware.com/download/esx/esx201-11429update.html
- Mise à jour de sécurité pour "VMware ESX Server 1.5.2" :
  http://www.vmware.com/download/esx/esx152-10816update.html

Gestion détaillée du document

05 août 2004 version initiale.
30 août 2004 ajout référence aux bulletins de sécurité de SuSE, Gentoo et Mandrake.
20 janvier 20005 ajout référence aux mises à jour de sécurité VMware.