Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 janvier 2004
N° CERTA-2004-AVI-002-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du noyau linux

Gestion du document

Référence	CERTA-2004-AVI-002-001
Titre	Vulnérabilité du noyau linux
Date de la première version	07 janvier 2004
Date de la dernière version	09 janvier 2004
Source(s)	Bulletin de sécurité isec-0013-mremap d'Isec Bulletin de sécurité SuSE-SA-2004:001 de SuSE Bulletin de sécurité RHSA-2003:417 de Red Hat BUlletin de sécurité DSA-413 de Debian
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.

2 Systèmes affectés

- Linux 2.4.23 et versions antérieures ;
- linux 2.6.1-rc1 et versions antérieures.

3 Description

Il a été reporté qu'une vulnérabilité présente dans l'appel système `mremap` du noyau Linux pourrait être exploitée par un utilisateur mal intentionné afin d'obtenir les privilèges du super-utilisateur `root` ou réaliser un déni de service par arrêt brutal du système.

4 Solution

Les versions 2.4.24 et 2.6.1-rc3 du noyau Linux corrigent cette vulnérabilité.

5 Documentation

- Bulletin de sécurité isec-0013-mremap d'Isec :
  http://isec.pl/vulnerabilities/isec-0013-mremap.txt
- Sources du noyau Linux :
  http://www.kernel.org
- Bulletin de sécurité DSA-413 de Debian :
  http://www.debian.org/security/2004/dsa-413
- Bulletin de sécurité RHSA-2003:417 de Red Hat :
  http://rhn.redhat.com/errata/RHSA-2003-417.html
- Bulletin de sécurité SuSE-SA:2004:01 de SuSE :
  http://www.suse.com/de/security/2004_01_linux_kernel.html
- Bulletin de sécurité MDKSA-2004:001 de Mandrake :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:001
- Bulletin de sécurité GLSA 200401-01 de Gentoo :
  http://marc.theaimsgroup.com/?l=gentoo-announce&m=107360666507658
- Référence CVE CAN-2003-0985 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0985

Gestion détaillée du document

07 janvier 2004 version initiale.

09 janvier 2004 Modification de la version du correctif pour les noyaux de la série 2.6. Ajout références aux bulletins de sécurité de Gentoo et Mandrake.