Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 juillet 2003
N° CERTA-2003-AVI-087-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans le noyau linux 2.4

Gestion du document

Référence	CERTA-2003-AVI-087-001
Titre	Vulnérabilités dans le noyau linux 2.4
Date de la première version	16 mai 2003
Date de la dernière version	24 juillet 2003
Source(s)	Bulletin de sécurité RHSA-2003:172-23 de Red Hat
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 ;
- élévation de privilèges.

2 Systèmes affectés

- Red Hat Linux 7.1 ;
- Red Hat Linux 7.2 ;
- Red Hat Linux 7.3 ;
- Red Hat Linux 8.0 ;
- Red Hat Linux 9 ;
- Mandrake 8.2 ;
- Mandrake 9.0 ;
- Mandrake Multi Network Firewall 8.2 ;
- Mandrake Corporate Server 2.1 ;
- Debian utilisant un noyau de la série 2.4.

3 Résumé

Plusieurs vulnérabilités sont présentes dans le noyau linux 2.4.

4 Description

- Une vulnérabilité présente dans la mise en oeuvre de plusieurs tables de hachage réseau du noyau Linux permet à un utilisateur mal intentionné d'effectuer un déni de service par l'envoi massif de paquets malicieux ;
- L'appel système `ioperm` permet d'appliquer les permissions sur les ports d'entrées/sorties. Une vulnérabilité présente dans celui-ci permet à un utilisateur local d'obtenir un accès en lecture et écriture aux ports d'entrées/sorties du système.

5 Solution

Appliquer le correctif suivant la version affectée :

- Bulletin de sécurité #RHSA-2003:172-23 de Red Hat :
  http://rhn.redhat.com/errata/RHSA-2003-172.html
- Bulletin de sécurité #RHSA-2003:187-25 de Red Hat :
  http://rhn.redhat.com/errata/RHSA-2003-187.html
- Bulletin de sécurité #RHSA-2003:195-06 de Red Hat :
  http://rhn.redhat.com/errata/RHSA-2003-195.html
- Bulletin de sécurité #MDKSA-2003:066-01 de Mandrake :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2003:066-1
- Bulletin de sécurité #MDKSA-2003:074 de Mandrake :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2003:074
- Bulletin de sécurité #DSA 311-1 de Debian :
  http://www.debian.org/security/2003/dsa-311
- Bulletin de sécurité #DSA 332-1 de Debian :
  http://www.debian.org/security/2003/dsa-332

6 Documentation

- Référence CVE CAN-2003-0244 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0244
- Référence CVE CAN-2003-0246 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0246

Gestion détaillée du document

16 mai 2003 version initiale.

24 juillet 2003 ajout des bulletins de sécurité Mandrake, RedHat et Debian.