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-118

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans le noyau linux 2.4

Gestion du document

Référence	CERTA-2003-AVI-118
Titre	Multiples vulnérabilités dans le noyau linux 2.4
Date de la première version	24 juillet 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité #RHSA-2003:238 de RedHat
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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Red Hat Linux 7.x, 8.0 et 9 ;
- Mandrake 9.1.

3 Résumé

Plusieurs vulnérabilités ont été découvertes dans le noyau linux 2.4.

4 Description

- Une vulnérabilité dans `/proc/tty/driver/serial` permet à un utilisateur mal intentionné d'obtenir des informations sur les mots de passe des utilisateurs locaux ;

- l'appel système `execve` permet d'exécuter des programmes. Celui-ci présente une vulnérabilité permettant d'effectuer un déni de service sur la machine ;
- RPC (Remote Procedure Call) est un protocole de type client/serveur utilisé pour l'implémentation d'applications réparties. Une vulnérabilité dans sa mise en oeuvre permet à un individu mal intentionné de perturber les services RPC ;
- une vulnérabilité dans l'appel système `execve` permet d'obtenir un accès en lecture à des descripteurs de fichier ayant un accès restreint ;
- une vulnérabilité dans le système de fichier `/proc` permet à un utilisateur local d'obtenir des informations sensibles ;
- le protocole STP (Spanning Tree Protocol) est utilisé afin d'éviter les problèmes de boucles sur un réseau. Celui-ci est installé par défaut dans le noyau 2.4 et peut être utilisé par un individu mal intentionné afin de modifier la topologie des ponts ;
- une mauvaise gestion des données reçues par le protocole STP permet d'effectuer un déni de service ;
- une vulnérabilité permet à un individu mal intentionné d'altérer le fonctionnement de la table de relayage (Forwarding Table).

5 Solution

Appliquer les correctifs fournis par l'éditeur (cf. Documentation).

6 Documentation

Bulletin de sécurité #RHSA-2003-238 de RedHat :
http://www.redhat.com/support/errata/RHSA-2003-238.html
Bulletin de sécurité #MDKSA-2003:066-1 de Mandrake :
http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:066-1
Référence CVE CAN-2003-0461 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0461
Référence CVE CAN-2003-0462 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0462
Référence CVE CAN-2003-0464 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0464
Référence CVE CAN-2003-0476 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0476
Référence CVE CAN-2003-0501 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0501
Référence CVE CAN-2003-0550 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0550
Référence CVE CAN-2003-0551 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0551
Référence CVE CAN-2003-0552 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0552

Gestion détaillée du document

24 juillet 2003 version initiale.