Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 mars 2003
N° CERTA-2003-AVI-051-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des noyaux Linux 2.2 et 2.4

Gestion du document

Référence	CERTA-2003-AVI-051-002
Titre	Vulnérabilité des noyaux Linux 2.2 et 2.4
Date de la première version	18 mars 2003
Date de la dernière version	28 mars 2003
Source(s)	–
Pièce(s) jointe(s)	Aucune

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

1 Risque

Usurpation des privilèges du super-utilisateur (*root*) en local.

2 Systèmes affectés

Toute distribution Linux utilisant un noyau de la série 2.2 jusqu'au 2.2.24 inclus ou de la série 2.4 jusqu'au 2.4.20 inclus.

3 Résumé

Un utilisateur mal intentionné, connecté localement, peut obtenir tous les privilèges du système.

4 Description

L'appel système *ptrace* du noyau Linux fournit le moyen pour un processus parent d'observer et contrôler l'éxécution d'un autre processus, et d'éditer son image mémoire. Cette fonction est principalement utilisée pour gérer les points d'arrêts dans les opérations de débogage.

Une faille dans cet appel peut être exploitée pour disposer des privilèges de l'utilisateur *root*.

5 Solution

- Mettre à jour le noyau Linux à partir des sources :
  - Série 2.2, mettre à jour en version 2.2.25 au moins :
    ftp://www.kernel.org/pub/linux/kernel/v2.2/
  - Série 2.4, mettre à jour en version 2.4.21-pre6 au moins :
    ftp://www.kernel.org/pub/linux/kernel/v2.4/testing/
- Distributions Red Hat Linux 7.1, 7.2, 7.3 et 8.0 :
  https://rhn.redhat.com/errata/RHSA-2003-098.html
- Gentoo Linux :
  http://forums.gentoo.org/viewtopic.php?t=42814
- Openwall :
  http://www.openwall.com/linux/
- Trustix Secure Linux 1.01, 1.1, 1.2 et 1.5 :
  http://www.trustix.net/errata/misc/2003/TSL-2003-0007-kernel.asc.txt
- EnGarde :
  http://www.linuxsecurity.com/advisories/engarde_advisory-2976.html
- Turbolinux :
  http://www.turbolinux.com/security/TLSA-2003-17.txt
- SuSE :
  http://www.suse.com/de/security/2003_21_kernel.html
- Mandrake :
  - série 2.4 :
    http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:038
  - série 2.2 :
    http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:039
- Debian :
  - architecture Mips :
    http://www.debian.org/security/2003/dsa-270

6 Documentation

- Message d'Alan Cox dans la liste de diffusion des développeurs du noyau Linux :
  http://www.uwsg.indiana.edu/hypermail/linux/kernel/0303.2/0226.html
- Annonce de la sortie du noyau linux 2.4.21-pre6 :
  http://marc.theaimsgroup.com/?l=linux-kernel&m=104872392328305&w=2
- Référence CVE CAN-2003-0127 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0127

Gestion détaillée du document

18 mars 2003 version initiale.

25 mars 2003 ajout de la référence CVE et des distributions Gentoo,

28 mars 2003 correction liste systèmes affectés. Ajout avis Debian (DSA-270), Mandrake, SuSE. Ajout lien sur kernel 2.4.21-pre6.