Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 juin 2005
N° CERTA-2005-AVI-174-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples failles des noyaux Linux

Gestion du document

Référence	CERTA-2005-AVI-174-003
Titre	Multiples failles des noyaux Linux
Date de la première version	24 mai 2005
Date de la dernière version	17 juin 2005
Source(s)	
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,
- déni de service local et distant,
- exécution locale de code arbitraire.

2 Systèmes affectés

Potentiellement tout système utilisant un noyau Linux en versions 2.2, 2.4 ou 2.6.

3 Résumé

Plusieurs failles ont été identifiées dans le code du noyau Linux et font l'objet de correctifs de la part des éditeurs.

4 Description

On peut recenser de nombreux correctifs, variables avec les éditeurs, les plus critiques correspondant à des configurations courantes sont décrits ci-dessous :

- CAN-2005-0209 : l'architecture de filtrage *netfilter* gère mal certaines cartes réseau et un déni de service peut être obtenu à l'aide de paquets IP fragmentés volontairement mal formés.
- CAN-2005-0400 : une mauvaise initialisation lors de la création d'un répertoire sous le système de fichiers *ext2* divulgue des données de l'espace noyau qui peuvent s'avérer sensibles.
- CAN-2005-0449 : une mauvaise gestion de la file d'attente des paquets fragmentés permet à un utilisateur mal intentionné d'effectuer un déni de service moyennant une connaissance des règles de filtrage configurées dans *netfilter*.
- CAN-2005-0529 : il est possible de réaliser un débordement de tampon dans la pile en accédant au pseudo système de fichiers *proc*.
- CAN-2005-0530 : il est possible de lire la mémoire du noyau suite à une erreur dans le gestionnaire de terminal.
- CAN-2005-0749 : un utilisateur local mal intentionné peut tenter d'exécuter un programme, au format standard ELF, volontairement mal formé pour provoquer un accès mémoire illégal et bloquer le noyau.
- CAN-2005-0750 : une faille dans la pile du gestionnaire de protocole sans fil Bluetooth peut être utilisée pour exécuter du code arbitraire avec les privilèges (tous) du noyau.
- CAN-2005-0815 : un cédérom avec un système de fichiers standard ISO-9660 volontairement mal formé peut provoquer un déni de service, voire provoquer l'exécution de code arbitraire, lors de son montage.
- CAN-2005-1041 : un utilisateur local mal intentionné peut provoquer un déni de service moyennant l'accès au pseudo-fichier `/proc/net/route`.
- CAN-2005-1263 : un fichier binaire ELF volontairement mal formé permet d'exécuter du code arbitraire avec les privilèges du noyau lors d'un vidage mémoire (« coredump » souvent autorisé pour les utilisateurs courants).
- CAN-2005-1264 : l'accès pour un utilisateur local à un périphérique de type caractère en mode brut (« raw ») peut être utilisé pour modifier l'espace du noyau avec le risque d'exécution de code arbitraire.
- CAN-2005-1589 : un problème identique existe dans le gestionnaire de type bloc des graveurs de cédéroms et dévédéroms.

5 Solution

Consulter le bulletin de l'éditeur pour l'obtention d'un correctif (cf. section Documentation).

6 Documentation

- Les sources du noyau Linux 2.6.11.10 et postérieures corrigent ces vulnérabilités :
  http://www.kernel.org
- Référence CVE CAN-2005-0209 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0209
- Référence CVE CAN-2005-0400 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0400
- Référence CVE CAN-2005-0449 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0449
- Référence CVE CAN-2005-0529 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0529
- Référence CVE CAN-2005-0530 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0530
- Référence CVE CAN-2005-0749 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0749
- Référence CVE CAN-2005-0750 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0750

- Référence CVE CAN-2005-0815 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0815
- Référence CVE CAN-2005-1041 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1041
- Référence CVE CAN-2005-1263 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1263
- Référence CVE CAN-2005-1264 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1264
- Référence CVE CAN-2005-1589 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1589
- Bulletins de sécurité Red Hat Linux :
  - versions 2.1, RHSA-2005:283 et RHSA-2005:284 du 28 avril 2005 :
    http://rhn.redhat.com/errata/RHSA-2005-283.html
    http://rhn.redhat.com/errata/RHSA-2005-284.html
  - versions 3, RHSA-2005:293 du 22 avril 2005 et RHSA-2005:472 du 25 mai 2005 :
    http://rhn.redhat.com/errata/RHSA-2005-293.html
    http://rhn.redhat.com/errata/RHSA-2005-472.html
  - versions 4, RHSA-2005:366 du 19 avril 2005 :
    http://rhn.redhat.com/errata/RHSA-2005-366.html
- Bulletins de sécurité SuSE SUSE-SA:2005:018 du 24 mars 2005, SUSE-SA:2005:021 du 04 avril 2005 et SUSE-SA:2005:029 du 09 juin 2005 :
  http://www.novell.com/linux/security/advisories/2005_018_kernel.html
  http://www.novell.com/linux/security/advisories/2005_021_kernel.html
  http://www.novell.com/linux/security/advisories/2005_029_kernel.html
- Gentoo Linux : la version gentoo-sources-2.6.11-r9 inclut les correctifs pour l'ensemble de ces failles.
- Bulletin de sécurité Avaya ASA-2005-120 du 2 juin 2005 :
  http://support.avaya.com/elmodocs2/security/ASA-2005-120_RHSA-2005-283_RHSA-2005-284_RHSA-2005-293_RHSA-2005-472.pdf

Gestion détaillée du document

24 mai 2005 version initiale ;

27 mai 2005 ajout du bulletin de sécurité Red Hat RHSA-2005:472 ;

14 juin 2005 ajout du bulletin de sécurité Novell SUSE-SA:2005:029 ;

17 juin 2005 ajout du bulletin de sécurité Avaya ASA-2005-120.