



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 janvier 2005
N° CERTA-2004-AVI-409-005

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Nombreuses failles du noyau Linux

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-409>

Gestion du document

Référence	CERTA-2004-AVI-409-005
Titre	Nombreuses failles du noyau Linux
Date de la première version	20 décembre 2004
Date de la dernière version	20 janvier 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

- Exécution de code arbitraire à distance ;
- élévation de privilèges ;
- déni de service ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Tout système d'exploitation utilisant un noyau Linux.

3 Résumé

Plusieurs vulnérabilités, décrites ci-dessous, affectent les noyaux Linux des séries 2.4 et/ou 2.6.

4 Description

4.1 Vulnérabilité du système de fichiers Samba

Références CVE CAN-2004-0883 et CAN-2004-0949.

Il est possible, pour un utilisateur mal intentionné contrôlant un serveur Samba, de provoquer un déni de service sur la station cliente sous Linux. Il n'est pas établi que l'exécution de code arbitraire à distance ou localement soit impossible.

4.2 Déni de service local sur les «sockets» Unix

Référence CVE-CAN-2004-1016.

Un utilisateur local mal intentionné peut transmettre des données volontairement mal formées qui seront mal interprétées et bloqueront le noyau.

4.3 Atteinte à la confidentialité des variables d'environnement

Référence CVE CAN-2004-1058.

Les variables d'environnement peuvent être utilisées pour passer des informations sensibles à un processus. C'est pourquoi leur consultation à travers le pseudo-système de fichier *proc* est restreinte. Cependant leur contenu est parfois visible dans la ligne de commande donc la lecture est plus permissive.

4.4 Exécution locale de code arbitraire avec les «sockets» Unix

Références CVE-CAN-2004-1068 et CVE-CAN-2004-1069.

Des conditions de concurrence peuvent être utilisées pour :

- modifier une portion arbitraire de la mémoire du noyau et ainsi élever les privilèges d'un utilisateur local (CVE-CAN-2004-1068) ;
- provoquer un déni de service (CVE-CAN-2004-1069).

4.5 Déni de service local avec un exécutable «a.out»

Référence CVE-CAN-2004-1074.

«a.out» est l'ancien format des exécutables sous Linux. Il a depuis été remplacé par le format ELF. Cependant la compatibilité avec ce format est souvent incluse dans le noyau. L'exécution d'un binaire de ce type, volontairement mal formé, peut provoquer un déni de service du noyau.

4.6 Mauvaise gestion du protocole IGMP

Références CVE-CAN-2004-1137.

IGMP («Internet Group Management») est un protocole IP utilisé pour offrir des communications «multicast». Il est en particulier utilisé par des applications de vidéoconférence ou de gestion dynamique du routage.

Il est possible pour un utilisateur local mal intentionné d'exécuter un programme qui provoquera un déni de service voire une élévation de privilèges.

Par ailleurs, si une application écoute sur une «socket multicast», il est possible, sous certaines conditions, de bloquer l'exécution du noyau.

4.7 Débordements de tampon dans le code des AMD 64 bits

Référence CVE-CAN-2004-1151.

4.8 Déni de service local dans la gestion des options IP et des terminaux virtuels

Deux fonctions du noyau gérant mal les débordements d'entier ont été identifiées. Elles peuvent être détournées pour provoquer un déni de service du noyau par un utilisateur local exécutant du code malicieux.

4.9 Débordement de mémoire dans la gestion des appels systèmes 32 bits sur plates-formes x86-64

Référence CVE-CAN-2004-1144.

La vulnérabilité est présente dans le noyau 2.4 uniquement et pour les plates-formes x86-64.

La version 2.4.29-pre3 corrige cette vulnérabilité.

4.10 Dénier de service local avec un exécutable «elf» pour les noyaux 2.4.x

Référence CVE-CAN-2004-1234.

«elf» est le format des exécutables sous Linux. Au moyen d'un fichier habilement constitué, un utilisateur mal intentionné peut provoquer un déni de service par arrêt brutal du système.

La version 2.4.28-rc4 corrige cette vulnérabilité.

5 Solution

Les noyaux «vanilla» jusqu'aux versions 2.6.9 et 2.4.28 sont vulnérables à au moins l'une des failles décrites ci-dessus ; utiliser une version en développement ou se référer aux bulletins de sécurité des éditeurs pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

6.1 Sources du noyau Linux

<http://www.kernel.org>

6.2 Vulnérabilité du système de fichiers Samba

- Références CVE CAN-2004-0883 et CAN-2004-0949 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0883>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0949>
- Bulletin de sécurité eMatters du 17 novembre 2004 :
<http://security.e-matters.de/advisories/142004.html>
- Bulletin de sécurité Secunia SA13232 du 18 novembre 2004 :
<http://secunia.com/advisories/13232/>

6.3 Dénier de service local sur les «sockets» Unix

- Référence CVE-CAN-2004-1016 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1016>
- Bulletin de sécurité Isec Security Research du 14 décembre 2004 :
<http://isec.pl/vulnerabilities/isec-0019-scm.txt>
- Bulletin de sécurité Secunia SA13469 du 15 décembre 2004 :
<http://secunia.com/advisories/13469/>

6.4 Atteinte à la confidentialité des variables d'environnement

- Référence CVE CAN-2004-1058 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1058>

6.5 Exécution locale de code arbitraire avec les «sockets» Unix

- Références CVE-CAN-2004-1068 et CVE-CAN-2004-1069 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1068>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1069>
- Bulletin de sécurité Secunia SA13232 du 18 novembre 2004 :
<http://secunia.com/advisories/13232/>

6.6 Dénis de service local avec un exécutable «a.out»

- Référence CVE-CAN-2004-1074 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1074>

6.7 Mauvaise gestion du protocole IGMP

- Références CVE-CAN-2004-1137 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1137>
- Bulletin de sécurité Isec Security Research du 14 décembre 2004 :
<http://isec.pl/vulnerabilities/isec-0018-igmp.txt>
- Bulletin de sécurité Secunia SA13469 du 15 décembre 2004 :
<http://secunia.com/advisories/13469/>

6.8 Débordements de tampon dans le code des AMD 64 bits

- Référence CVE-CAN-2004-1151 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1151>
- Bulletin de sécurité Secunia SA13410 du 09 décembre 2004 :
<http://secunia.com/advisories/13410/>

6.9 Dénis de service local dans la gestion des options IP et des terminaux virtuels

- Bulletin de sécurité #72 du Georgi Guninski :
http://www.guninski.com/where_do_you_want_billg_to_go_today_2.html
- Bulletin de sécurité Secunia SA13493 du 17 décembre 2004 :
<http://secunia.com/advisories/13493/>

6.10 Débordement de mémoire dans la gestion des appels systèmes 32 bits sur plateformes x86-64

- Référence CVE-CAN-2004-1144 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1144>
- Message "[PATCH] [CAN-2004-1144] Fix int 0x80 hole in 2.4 x86-64 linux kernels" :
<http://www.ussg.iu.edu/hypermail/linux/kernel/0412.2/1364.html>

6.11 Dénis de service local avec un exécutable «elf»

- Référence CVE-CAN-2004-1234 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1234>
- Correctifs inclus dans la version 2.4.28-rc4 du noyau :
<http://www.kernel.org/pub/linux/kernel/v2.4/Changelog-2.4.28>

6.12 Bulletin de sécurité des éditeurs

- Bulletin de sécurité RedHat RHSA-2004:549 du 02 décembre 2004 (CAN-2004-0883, CAN-2004-949 et CAN-2004-1068) :
<http://rhn.redhat.com/errata/RHSA-2004-549.html>
- Bulletin de sécurité SUSE SuSE-SA:2004:042 du 01 décembre 2004 (CAN-2004-0883, CAN-2004-949 et CAN-2004-1074) :
http://www.novell.com/linux/security/advisories/2004_42_kernel.html
- Bulletin de sécurité SUSE SuSE-SA:2004:044 du 21 décembre 2004 (CAN-2004-1016, CAN-2004-1068, CAN-2004-1137 et CAN-2004-1151) :
http://www.novell.com/linux/security/advisories/2004_44_kernel.html
- Bulletin de sécurité SUSE SuSE-SA:2004:046 du 22 décembre 2004 (CAN-2004-1144) :
http://www.novell.com/linux/security/advisories/2004_46_kernel.html

- Bulletin de sécurité RedHat RHSA-2004:689 du 23 décembre 2004 : (CAN-2004-0565, CAN-2004-1016, CAN-2004-1017, CAN-2004-1037, CAN-2004-1144 et CAN-2004-1234) :
<http://rhn.redhat.com/errata/RHSA-2004-689.html>
- Bulletin de sécurité Avaya ASA-2005-006 (CAN-2004-0883, CAN-2004-0949, CAN-2004-1016, CAN-2004-1017, CAN-2004-1068, CAN-2004-1137, CAN-2004-1234) :
http://support.avaya.com/elmodocs2/security/ASA-2005-006_RHSA-2004-549RHSA-2004-505RHSA-2004-689.pdf
- Bulletin de sécurité RedHat RHSA-2005:043 du 18 janvier 2005 (CAN-2004-1016) :
<http://rhn.redhat.com/errata/RHSA-2005-043.html>

Gestion détaillée du document

20 décembre 2004 version initiale.

23 décembre 2004 ajout référence au bulletin de sécurité SUSE SuSE-SA:2004:044.

23 décembre 2004 deuxième mise-à-jour : ajout référence CVE CAN-2004-1144 et bulletin de sécurité SUSE associé.

04 janvier 2004 ajout référence au bulletin de sécurité RedHat RHSA-2004:689. Ajout référence CVE CAN-2004-1234.

17 janvier 2005 ajout référence au bulletin de sécurité Avaya ASA-2005-006.

20 janvier 2005 ajout référence au bulletin de sécurité RedHat RHSA-2005:043.