



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 janvier 2005
N° CERTA-2004-AVI-372-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des noyaux Linux 2.4 et 2.6

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-372>

Gestion du document

Référence	CERTA-2004-AVI-372-002
Titre	Vulnérabilité des noyaux Linux 2.4 et 2.6
Date de la première version	19 novembre 2004
Date de la dernière version	17 janvier 2005
Source(s)	Bulletin de sécurité iSEC Security Research
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 ;
- éventuelle exécution de code arbitraire.

2 Systèmes affectés

Tout système Linux utilisant un noyau original («vanilla») :

- 2.4 jusqu'au 2.4.27,
- 2.6 jusqu'au 2.6.9 ;

ou la version d'un éditeur non corrigée.

3 Résumé

Un utilisateur local pouvant exécuter des programmes SUID (« Set User ID ») *root* peut provoquer un déni de service. Il n'est pas exclu que l'exécution de code arbitraire avec les privilèges du super-utilisateur soit également possible.

4 Description

L'appel système *execve* est utilisé pour lancer un nouveau programme. Par ailleurs, les systèmes d'exploitation Linux récents utilisent le format d'exécutable ELF (« Executable and Linkable Format »). Pour ces programmes, *execve* appelle du code dédié pour charger en mémoire le binaire. Ce code ne valide pas bien certains appels et il est alors possible de leurrer le système quand au bon chargement du binaire.

Dans le cas des programmes SUID, le noyau va alors permettre l'exécution avec les droits *root* d'un code mal formé.

5 Contournement provisoire

Restreindre à des utilisateurs de confiance l'exécution de programmes SUID.

6 Solution

Mettre à jour le noyau « vanilla » en version 2.6.10 au moins ou se référer au bulletin de sécurité de l'éditeur.

7 Documentation

- Sources du noyau Linux :
<http://www.kernel.org>
- Bulletin de sécurité iSEC Security Research :
http://isec.pl/vulnerabilities/isec-0017-binfmt_elf.txt
- Bulletin de sécurité Secunia du 10 novembre 2004 :
<http://secunia.com/advisories/13126>
- Références CVE CAN-2004-1070, CAN-2004-1071, CAN-2004-1072 et CAN-2004-1073 du 29 novembre 2004 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1070>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1071>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1072>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1073>
- Bulletin de sécurité RedHat RHSA-2004:549-10 du 02 décembre 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-549.html>
- Bulletin de sécurité SUSE SuSE-SA:2004:042 du 01 décembre 2004 :
http://www.novell.com/linux/security/advisories/2004_42_kernel.html
- Bulletin de sécurité Avaya ASA-2005-006 :
http://support.avaya.com/elmodocs2/security/ASA-2005-006_RHSA-2004-549RHSA-2004-505RHSA-2004-689.pdf
- Les noyaux Gentoo ont été mis à jour courant novembre et, bien qu'aucun bulletin de sécurité n'ait été édité, un noyau postérieur au 1er décembre 2004 ne doit plus être vulnérable.

Gestion détaillée du document

19 novembre 2004 version initiale ;

20 décembre 2004 ajout des références CVE CAN-2004-1070, CAN-2004-1071, CAN-2004-1072 et CAN-2004-1073, des bulletins des éditeurs RedHat et SuSE et du statut de la distribution Gentoo.

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