



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 juillet 2004
N° CERTA-2004-AVI-131-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-131>

Gestion du document

Référence	CERTA-2004-AVI-131-002
Titre	Vulnérabilité du noyau linux
Date de la première version	15 avril 2004
Date de la dernière version	07 juillet 2004
Source(s)	Bulletin de sécurité 0.14.04 d'iDEFENSE
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

Elévation de privilèges.

2 Systèmes affectés

- Linux 2.4.25 et versions antérieures ;
- Linux 2.6.5 et versions antérieures.

3 Résumé

Une vulnérabilité présente dans le noyau Linux peut être exploitée par un utilisateur mal intentionné afin de réaliser une élévation de privilèges.

4 Description

Une vulnérabilité de type débordement de mémoire est présente dans deux fonctions du noyau Linux relatives à la gestion des liens symboliques du système de fichiers ISO9660.

Un utilisateur mal intentionné peut exploiter cette vulnérabilité afin de réaliser une élévation de privilèges.

5 Contournement provisoire

Pour les noyaux Linux modulaires, désactiver le chargement du module `isofs`.

6 Solution

Les versions 2.4.26 et 2.6.6-rc1 du noyau Linux corrigent cette vulnérabilité :
<http://www.kernel.org>

7 Documentation

- Bulletin de sécurité 04.14.04 d'iDEFENSE :
<http://www.idefense.com/application/poi/display?id=101&type=vulnerabilities>
- Bulletins de sécurité de Debian :
<http://www.debian.org/security/2004/dsa-479>
<http://www.debian.org/security/2004/dsa-480>
<http://www.debian.org/security/2004/dsa-481>
<http://www.debian.org/security/2004/dsa-482>
<http://www.debian.org/security/2004/dsa-482>
<http://www.debian.org/security/2004/dsa-482>
<http://www.debian.org/security/2004/dsa-482>
- Bulletin de sécurité Gentoo GLSA-200407-02 du 03 juillet 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200407-02.xml>
- Bulletin de sécurité MDKSA-2004:029 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:029>
- Bulletin de sécurité SuSE-SA:2004:09 de SuSE :
http://www.suse.com/de/security/2004_09_kernel.html
- Bulletin de sécurité RHSA-2004:166 pour Red Hat Linux :
<https://rhn.redhat.com/errata/RHSA-2004-166.html>
- Bulletin de sécurité RHSA-2004:183 pour Red Hat Enterprise Linux :
<https://rhn.redhat.com/errata/RHSA-2004-183.html>
- Référence CVE CAN-2004-0109 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0109>

Gestion détaillée du document

15 avril 2004 version initiale.

27 avril 2004 ajout références aux bulletins DSA-489, DSA-491, DSA-495 de Debian et RHSA-166, RHSA-183 de Red Hat.

07 juillet 2004 ajout référence au bulletin de sécurité Gentoo GLSA-200407-02.