

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-139>

Gestion du document

Référence	CERTA-2004-AVI-139-001
Titre	Vulnérabilité du noyau Linux
Date de la première version	21 avril 2004
Date de la dernière version	28 avril 2004
Source(s)	Bulletin de sécurité de Isec Security Research du 20 avril 2004
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 versions 2.4.22 à 2.4.25 ;
- Linux versions 2.6.1 à 2.6.3.

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 présente dans la fonction `ip_setsockopt()` peut être exploitée par un utilisateur mal intentionné afin de réaliser une élévation de privilèges.

5 Solution

Installer le noyau Linux à partir des sources, les versions 2.4.26 et 2.6.4 (ou versions supérieures) corrigeant cette vulnérabilité, ou appliquer le correctif fournit par l'éditeur :

- Bulletin de sécurité RHSA-2004:183 de Red Hat pour Red Hat Enterprise Linux :
<https://rhn.redhat.com/errata/RHSA-2004-183.html>
- Bulletin de sécurité MDKSA-2004:037 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:037>

6 Documentation

- Bulletin de sécurité de Isec Security Research du 20 avril 2004 :
<http://www.isec.pl/vulnerabilities04.html>
<http://www.isec.pl/vulnerabilities/isec-0015-msfilter.txt>
- Référence CVE CAN-2004-0424 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0424>
- Site Internet du noyau Linux :
<http://www.kernel.org>

Gestion détaillée du document

21 avril 2004 version initiale.

28 avril 2004 ajout références aux bulletins MDKSA-2004:037 de Mandrake et RHSA-2004:183 de Red Hat.