

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-2003-AVI-204>

Gestion du document

Référence	CERTA-2003-AVI-204-001
Titre	Vulnérabilité du noyau Linux
Date de la première version	2 décembre 2003
Date de la dernière version	5 décembre 2003
Source(s)	Bulletin de sécurité DSA-403 de Debian Bulletin de sécurité MDKSA-2003:110 de Mandrake Bulletin de sécurité RHSA-2003:392 de Red Hat
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 ;
- déni de service.

2 Systèmes affectés

Linux 2.4.22 et versions antérieures.

3 Description

Une vulnérabilité est présente dans la fonction `do_brk()` du noyau Linux (contrôle incorrect de l'adresse haute de la zone mémoire dynamique (TAS) du processus).

Un utilisateur mal intentionné peut exploiter cette vulnérabilité afin d'obtenir les privilèges du super-utilisateur `root` ou réaliser un déni de service par arrêt brutal du système.

4 Solution

La version 2.4.23 du noyau Linux corrige cette vulnérabilité.

5 Documentation

- Sources du noyau Linux :
<http://www.kernel.org>
- Bulletin de sécurité DSA-403 de Debian :
<http://www.debian.org/security/2003/dsa-403>
- Bulletin de sécurité MDKSA-2003:110 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:110>
- Bulletin de sécurité RHSA-2003:392 de Red Hat :
<http://rhn.redhat.com/errata/RHSA-2003-392.html>
- Bulletin de sécurité SuSE-SA:2003:049 de SuSE :
http://www.suse.com/de/security/2003_049_kernel.html
- Bulletin de sécurité GLSA 200312-02 de Gentoo :
<http://www.securityfocus.com/advisories/6143>
- Référence CVE CAN-2003-0961 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0961>

Gestion détaillée du document

2 décembre 2003 version initiale.

5 décembre 2003 ajout références aux bulletins de SuSE et Gentoo.