

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-042>

Gestion du document

Référence	CERTA-2004-AVI-042-005
Titre	Vulnérabilité du noyau linux
Date de la première version	18 février 2004
Date de la dernière version	06 avril 2004
Source(s)	Bulletin de sécurité isec-0014-mremap-unmap d'Isec
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 2.4.24 et versions antérieures ;
- Linux 2.6.2 et versions antérieures.

3 Description

Il a été reporté qu'une nouvelle vulnérabilité présente dans l'appel système `mremap` du noyau Linux pourrait être exploitée par un utilisateur mal intentionné afin d'obtenir les privilèges du super-utilisateur `root` ou réaliser un déni de service par arrêt brutal du système.

Cet appel système ne nécessitant pas de privilèges particuliers, n'importe quel utilisateur peut tenter d'exploiter cette faille.

Bien que similaire à la vulnérabilité présente dans l'avis CERTA-2004-AVI-002, il s'agit bien d'un nouveau problème de sécurité.

4 Solution

Les versions 2.4.25 et 2.6.3 du noyau Linux corrigent cette vulnérabilité.

5 Documentation

- Bulletin de sécurité isec-0014-mremap-unmap d’Isec :
<http://isec.pl/vulnerabilities/isec-0014-mremap-unmap.txt>
- Sources du noyau Linux :
<http://www.kernel.org>
- Bulletins de sécurité DSA-438, DSA-439, DSA-440, DSA-441, DSA-442, DSA-470 de Debian :
<http://www.debian.org/security/2004/dsa-438>
<http://www.debian.org/security/2004/dsa-439>
<http://www.debian.org/security/2004/dsa-440>
<http://www.debian.org/security/2004/dsa-441>
<http://www.debian.org/security/2004/dsa-442>
<http://www.debian.org/security/2004/dsa-470>
- Bulletin de sécurité RHSA-2004:065 de Red Hat :
<http://rhn.redhat.com/errata/RHSA-2004-065.html>
- Bulletin de sécurité SSA:2004-049-01 de Slackware :
<http://slackware.com/security/viewer.php?l=slackware-security&y=2004&m=slackware-security.541911>
- Bulletin de sécurité SuSE-SA:2004:005 de SuSE :
http://www.suse.com/de/security/2004_05_linux_kernel.html
- Bulletin de sécurité Mandrake MDKSA-2004:015 :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:015>
- Bulletin de sécurité SmoothWall :
<http://www.smoothwall.org/security/advisories/SWP-2004.002.html>
- Bulletin de sécurité GLSA 200403-02 de Gentoo :
<http://www.securityfocus.com/advisories/6428>
- Bulletin de sécurité de VMware pour ESX Server 2.0.1 :
<http://www.vmware.com/download/esx/esx201-7427update.html>
- Bulletin de sécurité de VMware pour ESX Server 2.0 :
<http://www.vmware.com/download/esx/esx20-7483update.html>
- Bulletin de sécurité de VMware pour ESX Server 1.5.2 :
<http://www.vmware.com/download/esx/esx152-7428update.html>
- Référence CVE CAN-2004-0077 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0077>

Gestion détaillée du document

18 février 2004 version initiale.

20 février 2004 Ajout références aux bulletins SuSE-SA:2004:005 et DSA-442.

25 février 2004 Ajout référence au bulletin Mandrake MDKSA-2004:015.

27 février 2004 Ajout référence au bulletin SmoothWall SWP-2004.002.

05 avril 2004 Ajout références aux bulletins Debian DSA-470 et Gentoo GLSA 200403-02.

06 avril 2004 Ajout références aux bulletins de VMware pour ESX Server.