



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 juillet 2003
N° CERTA-2003-AVI-109-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans nfs-utils

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-109>

Gestion du document

Référence	CERTA-2003-AVI-109-003
Titre	Vulnérabilité dans nfs-utils
Date de la première version	15 juillet 2003
Date de la dernière version	24 juillet 2003
Source(s)	Bulletin de sécurité #RHSA-2003:206-01 de RedHat Bulletin de sécurité #DSA 349-1 de Debian
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

- Exécution de code arbitraire à distance.
- déni de service.

2 Systèmes affectés

Toutes les versions de NFS Utils antérieures ou égales à la version 1.0.3.

3 Résumé

Une vulnérabilité a été découverte dans le démon mountd de NFS Utils.

4 Description

Une vulnérabilité de type débordement de mémoire a été découverte dans la fonction de journalisation `xlog` utilisée par le démon `mountd`. Un utilisateur mal intentionné peut exploiter cette vulnérabilité afin d'exécuter du code arbitraire à distance ou d'effectuer un déni de service à l'aide de requêtes RPC malicieusement formées.

5 Solution

Appliquer le correctif suivant l'éditeur (cf. Documentation).

6 Documentation

Bulletin de sécurité #RHSA-2003:206-01 de RedHat :

<http://www.redhat.com/support/errata/RHSA-2003-206.html>

Bulletin de sécurité #DSA 349-01 de Debian :

<http://lists.debian.org/debian-security-announce/debian-security-announce-2003/msg00146.html>

Bulletin de sécurité #SuSE-SA:2003:031 de SuSE :

http://www.suse.de/de/security/2003_031_nfs_utils.html

Bulletin de sécurité Slackware :

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2003&m=slackware-security.360362>

Bulletin de sécurité #MDKSA-2003:076 de Mandrake :

<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:076>

Référence CVE CAN-2003-0252 :

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0252>

Gestion détaillée du document

15 juillet 2003 version initiale.

16 juillet 2003 ajout des bulletins SuSE et Slackware.

16 juillet 2003 rectification du numero de la version vulnerable.

24 juillet 2003 ajout du bulletin Mandrake.