



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 mai 2004
N° CERTA-2004-AVI-172-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sur rpc.mountd sur Irix

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-172>

Gestion du document

Référence	CERTA-2004-AVI-172-001
Titre	Vulnérabilité sur rpc.mountd sur Irix
Date de la première version	21 mai 2004
Date de la dernière version	25 mai 2004
Source(s)	Avis de sécurité SGI
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

Déni de service.

2 Systèmes affectés

Irix 6.5.24

3 Résumé

Une vulnérabilité présente sur le service `rpc.mountd` sur Irix 6.5.24 permet à un utilisateur mal intentionné de réaliser un déni de service sur le service vulnérable.

4 Description

Le service `rpc.mountd` est le service RPC (Remote Procedure Call) chargé du montage des partitions NFS (Network File System). Une vulnérabilité présente dans le traitement des requêtes RPC permet à un utilisateur mal intentionné, via l'envoi de requêtes RPC malicieusement construites, de réaliser un déni de service sur le service `rpc.mountd` en entraînant celui-ci dans une boucle infinie.

5 Solution

Mettre à jour votre système ou appliquer le correctif disponible sur le site de SGI (cf. section documentation).

6 Documentation

- Avis de sécurité SGI :
<ftp://patches.sgi.com/support/free/security/advisories/20040503-01-P.asc>
- Référence CVE CAN-2004-0154 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0154>

Gestion détaillée du document

21 mai 2004 version initiale.

25 mai 2004 correction de la référence CVE.