

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de `rpc.mountd` sous SGI 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-2005-AVI-199>

Gestion du document

Référence	CERTA-2005-AVI-199
Titre	Vulnérabilités de <code>rpc.mountd</code> sous SGI IRIX
Date de la première version	09 juin 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité 20050601-01-P de 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

- Atteinte à l'intégrité des données ;
- déni de service.

2 Systèmes affectés

SGI IRIX versions 6.5.25, 6.5.26 et 6.5.27.

3 Description

`rpc.mountd` est un service permettant le montage depuis un serveur NFS de volumes distants.
`bigskip`

Selon SGI, deux vulnérabilités sont présentes dans le service `rpc.mountd` :

- CVE CAN-2005-139 : il est possible de contourner la limitation d'accès en lecture ;
- CVE CAN-2005-138 : un déni de service est possible lorsque les clients anonymes ne possèdent pas de résolution inverse du nom de machine.

4 Solution

Se référer au bulletin de sécurité de l'éditeur (cf. section Documentation) pour l'obtention des correctifs.

5 Documentation

- Bulletin de sécurité SGI 20050601-01-P du 09 juin 2005 :
<ftp://patches.sgi.com/support/free/security/advisories/20050601-01-P.asc>
- Référence CVE CAN-2005-0138 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0138>
- Référence CVE CAN-2005-0139 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0139>

Gestion détaillée du document

09 juin 2005 version initiale.