



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 16 octobre 2002  
N° CERTA-2002-AVI-230

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités sous 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-2002-AVI-230>

---

### Gestion du document

Référence	CERTA-2002-AVI-230
Titre	Multiples vulnérabilités sous IRIX
Date de la première version	16 octobre 2002
Date de la dernière version	–
Source(s)	Avis 20020903-02-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

Elévation de privilèges.

## 2 Systèmes affectés

Toutes les versions 6.5 de SGI IRIX jusqu'à la version 6.5.17 incluse.  
Les versions antérieures à la 6.5 n'étant plus maintenues, la vulnérabilité de ces systèmes n'est pas connue.

## 3 Résumé

De multiples vulnérabilités dans certaines commandes sous IRIX permettent une élévation de privilèges.

## 4 Description

Certaines commandes sont sujettes à des vulnérabilités permettant une élévation de privilèges :

– `rpcbind` suit les liens symboliques lorsque cette commande est invoquée avec l'option `-w` ;

- quelques fichiers du bureau sont modifiables par tous ;
- `uux`, qui a des droits `sgid`, est vulnérable à une attaque de type débordement de mémoire ;
- `fsr_efs` suit les liens symboliques ;
- la commande `mv`, lorsqu'elle est invoquée pour déplacer un répertoire, crée le répertoire avec des droits en écriture pour tous.

## 5 Solution

Appliquer les correctifs 4819 et 4820, ou passer en version 6.5.18 lorsque celle-ci sera disponible.

Les correctifs peuvent être téléchargés à l'adresse suivante :

<ftp://patches.sgi.com/support/free/security/patches>

## 6 Documentation

Avis 200209-03-02-P de SGI :

<ftp://patches.sgi.com/support/free/security/advisories/20020903-02-P>

## Gestion détaillée du document

16 octobre 2002 version initiale.