Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 janvier 2005
N° CERTA-2004-AVI-198-001

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

## Objet : Multiples vulnérabilités sous IRIX



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2004-AVI-198-001 |
| Titre | Multiples vulnérabilités sous IRIX |
| Date de la première version | 15 juin 2004 |
| Date de la dernière version | 17 janvier 2005 |
| Source(s) | Bulletin de sécurité 20040601-01-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

- Elévation de privilèges ;
- déni de service.

## 2 Systèmes affectés

SGI IRIX 6.5.24 et versions antérieures.

## 3 Description

`syssgi` est une primitive système spécifique au système d'exploitation IRIX de SGI.
Selon SGI, une vulnérabilité présente dans la primitive système `syssgi` appellée avec l'argument `SGI_IOPROBE` peut être utilisée par un utilisateur mal intentionné pour lire ou même écrire dans l'espace mémoire du noyau et réaliser ainsi une élévation de privilèges.

Deux vulnérabilités permettant de réaliser un déni de service local sont également présentes :

- faille dans `mapelf32exec()` (CVE CAN-2004-136) ;
- faille dans `init` (CAN-2004-137).

# 4 Solution

La version 6.5.25 d'IRIX corrige ces vulnérabilités.
Se référer au bulletin de sécurité de l'éditeur (cf. section Documentation) pour l'obtention des correctifs.

# 5 Documentation

- Bulletin de sécurité SGI 20040601-01-P du 14 juin 2004 :
  ftp://patches.sgi.com/support/free/security/advisories/20040601-01-P.asc
- Bulletin de sécurité Avaya ASA-2005-006 :
  http://support.avaya.com/elmodocs2/security/ASA-2005-006_RHSA-2004-549RHSA-2004-505RHSA-2004-689.pdf
- Référence CVE CAN-2004-0135 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0135
- Référence CVE CAN-2004-0136 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0136
- Référence CVE CAN-2004-0137 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0137

# Gestion détaillée du document

**15 juin 2004** version initiale.
**17 janvier 2005** ajout référence au bulletin de sécurité Avaya ASA-2005-006.