Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 mai 2001
N° CERTA-2001-AVI-054

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de ESP sous IRIX

Gestion du document

Référence	CERTA-2001-AVI-054
Titre	Vulnérabilité de ESP sous SGI IRIX
Date de la première version	15 mai 2001
Date de la dernière version	–
Source(s)	Bulletin 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

Accès `root` à distance.

2 Systèmes affectés

SGI IRIX 6.5.5 à 6.5.8.

3 Résumé

Une vulnérabilité du service `rpc.espd` permet à un utilisateur mal intentionné d'effectuer un débordement de mémoire à distance et d'acquérir les privilèges de `root`.

4 Description

ESP (*Embedded Support Partner*) est un outil de maintenance à distance inclus dans le système d'exploitation IRIX. Il est installé par défaut sur les versions 6.5.5 et supérieures.

Il est possible d'effectuer à distance un débordement de mémoire du *daemon* `rpc.espd` pouvant conduire à une compromission de `root`.

5 Contournement provisoire

- Supprimer le service `rpc.espd` s'il n'est pas utilisé.
- Rendre non exécutable le service `rpc.espd` en attendant d'appliquer le correctif ou la nouvelle version. Ce contournement est d'ailleurs la seule solution pour les versions 6.5.5 et 6.5.6 qui ne sont plus maintenues par SGI.

  1. `/bin/chmod -x /usr/etc/rpc.espd`
  2. relancer les services avec la commande :
     `/etc/killal -HUP inetd`

6 Solution

- Pour les versions 6.5.7 et 6.5.8 de SGI, appliquer le correctif de SGI N 4123 :
  ftp://patches.sgi.com/support/free/security/patches
- La version 2.0 de ESP n'est pas vulnérable, elle est installée par défaut sur la version 6.5.9 d'IRIX.

7 Documentation

L'avis de sécurité de SGI :
http://patches.sgi.com/support/free/security/advisories/20010501-01-P

Gestion détaillée du document

15 mai 2001 version initiale.