Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 juin 2002
N° CERTA-2002-AVI-118

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité rpc.passwd sous IRIX

Gestion du document

Référence	CERTA-2002-AVI-118
Titre	Vulnérabilité rpc.passwd sous IRIX
Date de la première version	05 juin 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité #20020601-01-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.

2 Systèmes affectés

IRIX versions 6.5 à 6.5.15.

3 Résumé

Une vulnérabilité dans le serveur rpc.passwd peut permettre à un individu mal intentionné d'obtenir les privilèges du compte `root`.

4 Description

`NIS` (Network Information Service) est un service utilisé pour la centralisation des informations relatives aux comptes utilisateur du réseau.

yppasswd permet aux utilisateurs de modifier leur mot de passe. Ces modifications sont alors gérées par le service rpc.passwd.

Une vulnérabilité présente dans le démon rpc.passwd peut permettre à un individu mal intentionné d'obtenir les privilèges du compte `root`.

5 Contournement provisoire

Il est possible de désactiver le démon rpc.passwd :

```
chmod 444 /usr/etc/rpc.passwd
killall rpc.passwd
```

Ceci aura pour conséquence d'empêcher les utilisateurs de modifier leur mot de passe à distance.

6 Solution

Se référer au bulletin de SGI afin d'appliquer le correctif suivant la version affectée (cf. Documentation).

7 Documentation

Bulletin de sécurité #20020601-01-P de SGI :
http://www.sgi.com/support/security

Gestion détaillée du document

05 juin 2002 version initiale.