



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 décembre 2002
N° CERTA-2002-AVI-262

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de `priocntl` sous Solaris

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-262>

Gestion du document

Référence	CERTA-2002-AVI-262
Titre	Vulnérabilité de <code>priocntl</code> sous Solaris
Date de la première version	11 décembre 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité #49131 de Sun
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.
Cette vulnérabilité n'est pas exploitable à distance.

2 Systèmes affectés

Solaris 2.5.1 à 9.

3 Résumé

Une vulnérabilité présente dans la primitive système `priocntl` permet à un utilisateur mal intentionné d'obtenir les privilèges de l'administrateur système (`root`) sur une machine vulnérable.

4 Description

La primitive système `priocntl` est utilisée pour contrôler les paramètres d'ordonnancement d'un processus léger.

Une vulnérabilité présente dans la gestion de certains arguments fournis lors de l'appel à cette primitive permet à un utilisateur non privilégié de charger un module au niveau du noyau permettant ainsi de réaliser une élévation de privilèges.

5 Contournement provisoire

Se référer au bulletin de l'éditeur (section Documentation).

6 Solution

Se référer au bulletin de l'éditeur (section Documentation).

7 Documentation

- Bulletin de sécurité #49131 de Sun :
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F49131>
- Note VU#683673 du CERT/CC :
<http://www.kb.cert.org/vuls/id/683673>

Gestion détaillée du document

11 décembre 2002 version initiale.