Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 mai 2002
N° CERTA-2002-AVI-095

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités d'admintool sous Solaris

Gestion du document

Référence	CERTA-2002-AVI-095
Titre	Vulnérabilités d'admintool sous Solaris
Date de la première version	03 mai 2002
Date de la dernière version	–
Source(s)	Bulletin Sun Alert Notification #27353
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

Solaris versions 2.5, 2.5.1, 2.6, 7 et 8.

3 Résumé

De multiples vulnérabilités présentes dans l'outil `admintool` permettent à un utilisateur mal intentionné d'exécuter du code arbitraire avec les privilèges de l'administrateur `root`.

4 Description

L'utilitaire `admintool` est un outil d'administration (gestion des utilisateurs, installation de paquetages logiciels ...) utilisé sous Solaris.

De multiples vulnérabilités de type débordement de mémoire présentes dans l'outil `admintool` permettent à un utilisateur mal intentionné d'exécuter du code arbitraire avec les privilèges de l'administrateur `root`.

Ces vulnérabilités ne sont exploitables qu'en local.

5 Contournement provisoire

Si le correctif ne peut être appliqué immédiatement, retirer le drapeau `setuid` afin de prévenir l'exploitation de ces vulnérabilités :

```
# chmod u-s /usr/bin/admintool
```

6 Solution

Appliquer les correctifs (se référer à la section Documentation).

7 Documentation

- Bulletin Sun Alert Notification #27353 :
  http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F27353&zone_32=category%3Asecurity
- Avis eSO:2397 d'eSecurityOnline :
  http://www.eSecurityOnline.com/advisories/eSO2397.asp

Gestion détaillée du document

03 mai 2002 version initiale.