Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 décembre 2001
N° CERTA-2001-AVI-161-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de l'exécutable login

Gestion du document

Référence	CERTA-2001-AVI-161-001
Titre	Vulnérabilité de l'exécutable login
Date de la première version	13 décembre 2001
Date de la dernière version	19 décembre 2001
Source(s)	Avis CA-2001-34 du CERT/CC
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

- IBM AIX versions 4.3 et 5.1 ;
- SCO OpenServer version 5.0.6 et antérieures ;
- SGI IRIX 3.x ;
- Sun Solaris versions 2.5.1, 2.6, 7 et 8.

3 Résumé

Une vulnérabilité de l'exécutable */bin/login* permet à un utilisateur mal intentionné d'obtenir à distance les privilèges de l'administrateur *root*.

4 Description

Une vulnérabilité de type débordement de mémoire dans l'exécutable */bin/login* permet à un utilisateur d'obtenir les privilèges de l'administrateur *root*.

La fonction *login* n'est pas *suid* ; elle s'exécute donc avec les droits de celui qui l'appelle. Néanmoins, certaines applications, *rlogind* ou *telnetd* par exemple, fonctionnent avec les droits de *root* et font appel à *login*.

Il est alors possible par ce biais d'obtenir les droits de l'administrateur de la machine à distance.

5 Contournement provisoire

Limitez l'accès aux ports suivants sur les gardes-barrières :

- 23/tcp (*telnet*)
- 513/tcp (*rlogin*)

6 Solution

Contactez votre distributeur pour obtenir une mise à jour.

Pour les systèmes SGI IRIX, il est conseillé d'évoluer vers une versions d'IRIX parmi les versions 4.x, 5.x ou 6.x, qui ne sont pas vulnérables.

Pour les systèmes Sun, se reporter à l'avis 41987 (cf. Documentation) et appliquer les correctifs suivant la version et l'architecture du système.

7 Documentation

Avis CA-2001-34 du CERT/CC :
http://www.cert.org/advisories/CA-2001-34.html
Alerte Sun 41987 :
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=salert%2F41987&zone_32=41987
Avis SGI :
ftp://patches.sgi.com/support/free/security/advisories/20011201-01-I

Gestion détaillée du document

13 décembre 2001 version initiale.

19 décembre 2001 première révision : précision des versions vulnérables de Solaris et ajout des alertes SUN et SGI.