

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans les programmes et librairies d'impression 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-2000-AVI-024>

Gestion du document

Référence	CERTA-2000-AVI-024
Titre	Vulnérabilités dans les programmes et librairies d'impression sous Solaris
Date de la première version	08 août 2000
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Sun Bugtraq Avis du CERT IST
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

Exécution de code arbitraire permettant à un utilisateur local l'accès aux privilèges *root*.

2 Systèmes affectés

SunOS, Solaris.

3 Résumé

Plusieurs débordements de piles ont été détectés dans les librairies et les programmes d'impressions de Solaris. Ils permettent à un utilisateur local d'exécuter du code et d'obtenir les privilèges *root*.

Des exploitations de ces vulnérabilités ont été largement diffusées sur internet.

4 Description

L'utilitaire `lpset` permet de mettre les informations de configuration de l'imprimante dans la base de données de configuration du système. Cet outil utilise la librairie `libprint.so.2` qui présente une faille. Un utilisateur local mal intentionné peut exécuter du code grâce à un dépassement de mémoire de la commande `lpset -r` à une zone mémoire tampon habilement construite (l'option `-r` de `lpset` n'est pas documentée, donc peu connue).

Un autre débordement de pile est possible dans l'exécutable `/usr/lib/lp/bin/netpr` utilisée par les commandes d'impression pour envoyer les données vers une imprimante en passant par un réseau.

Il en est de même avec la commande beaucoup plus connue : `lp` suivie de l'option `-d`

L'utilisateur mal intentionné peut, dans chacun des cas, exécuter du code afin d'obtenir les privilèges `root`.

5 Contournement provisoire

Il est possible de supprimer le caractère *suid*, pour les commandes `lpset` et `lp` et `netpr`, mais cela aura pour effet d'en empêcher l'exécution par un utilisateur sans privilèges `root`.

```
chmod a-s `find / -name lp -print`
```

```
chmod a-s `find / -name lpset -print`
```

```
chmod a-s `find / -name netpr -print`
```

Sous Solaris 2.6, 2.7 et 2.8, une solution temporaire mais pas totalement efficace (car elle peut être contournée à son tour) consiste à inhiber l'exécution de code situé dans la pile. Pour cela, ajoutez les variables suivantes dans le fichier `/etc/system`:

```
set noexec_user_stack=1
```

```
set noexec_user_stack_log=1
```

Redémarrer la machine après avoir effectué cette modification.

6 Solution

Il faut appliquer les correctifs de Sun disponibles aux adresses suivantes :

- Sous Solaris 8
<http://sunsolve.sun.com/pub-cgi/patchDownload.pl?target=109320&method=F>
- Solaris 8_x86
<http://sunsolve.sun.com/pub-cgi/patchDownload.pl?target=109321&method=F>
- Solaris 7
<http://sunsolve.sun.com/pub-cgi/patchDownload.pl?target=107115&method=F>
- Solaris 7_x86
<http://sunsolve.sun.com/pub-cgi/patchDownload.pl?target=107116&method=F>
- Solaris 2.6
<http://sunsolve.sun.com/pub-cgi/patchDownload.pl?target=106235&method=F>
- Solaris 2.6_x86 (SunOS 5.6)
<http://sunsolve.sun.com/pub-cgi/patchDownload.pl?target=106236&method=F>
- Solaris 2.5.1
<http://sunsolve.sun.com/pub-cgi/patchDownload.pl?target=103948&method=F>

- Solaris 2.5 (SunOS 5.5)
<http://sunsolve.sun.com/pub-cgi/patchDownload.pl?target=102964&method=F>
- Solaris 2.5_x86
<http://sunsolve.sun.com/pub-cgi/patchDownload.pl?target=102959&method=F>
- Solaris 2.4 (SunOS 5.4)
<http://sunsolve.sun.com/pub-cgi/patchDownload.pl?target=101317&method=F>
- Solaris 2.4_x86
<http://sunsolve.sun.com/pub-cgi/patchDownload.pl?target=101962&method=F>

Ces correctifs, rectifient aussi d'autres erreurs dans l'implémentation de `lp`.

7 Documentation

Avis de sécurité de Sun concernant les débordements de pile des outils d'impression :

<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=coll&doc=secbull/195&type=0&nav=sec.sba>

Les avis de sécurité récents de Sun sont tous à cette adresse :

<http://sunsolve.sun.com/pub-cgi/secBulletin.pl>

Gestion détaillée du document

08 août 2000 version initiale.