



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 février 2007
N° CERTA-2007-ALE-005-002

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité de Sun 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-2007-ALE-005>

Gestion du document

Référence	CERTA-2007-ALE-005-002
Titre	Vulnérabilité de Sun Solaris
Date de la première version	12 février 2007
Date de la dernière version	18 septembre 2008
Source(s)	
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

Contournement de la politique de sécurité.

2 Systèmes affectés

- Sun Solaris 10;
- Sun Solaris Express.

3 Résumé

Une vulnérabilité permettant une connexion non légitime à distance a été découverte dans le système d'exploitation Sun Solaris.

4 Description

Une vulnérabilité a été découverte dans la conjonction du service `telnetd` et de la commande `/usr/cmd/login`. Cette vulnérabilité peut être exploitée par une personne distante afin de se connecter à la machine vulnérable sous

un nom d'utilisateur légitime, à condition d'en connaître un. Le système n'est cependant vulnérable qu'à la condition où le service `telnetd` soit démarré avec les droits `root`.

L'exploitation de cette vulnérabilité est triviale et un code d'exploitation circule sur l'Internet. D'autres services de connexion à distance présentent potentiellement le même type de vulnérabilité.

28 février 2007 : le CERTA a été informé de la propagation d'un ver exploitant cette vulnérabilité. Des méthodes pour le détecter sont fournies par Sun à l'adresse ci-dessous :

http://blogs.sun.com/security/entry/solaris_in_telnetd_worm_seen

5 Contournement provisoire

Désactiver le service `telnetd` grâce à la commande suivante :

```
svcadm disable telnetd
```

Par précaution, désactiver de la même manière les services `rlogind`, `klogin`, `eklogin` :

```
svcadm disable rlogind
```

```
svcadm disable klogin
```

```
svcadm disable eklogin
```

Il est également recommandé de vérifier que l'accès au port TCP 23 est correctement filtré au niveau des pare-feux, en accord avec la politique de sécurité.

6 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Bulletin de sécurité Sun #201391 du 28 février 2007 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102802-1>
- Référence CVE CVE-2007-0882 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0882>

Gestion détaillée du document

12 février 2007 version initiale.

28 février 2007 ajout d'informations concernant la propagation d'un ver et solution.

18 septembre 2008 passage en statut corrigé, ajout de la référence CVE.