Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 février 2005
N° CERTA-2005-AVI-080

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de 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-2005-AVI-080

Gestion du document

Référence	CERTA-2005-AVI-080
Titre	Multiples vulnérabilités de Solaris
Date de la première version	16 février 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité #57725 du 14 février 2005 de Sun Bulletin de sécurité #57673 du 14 février 2005 de Sun
Pièce(s) jointe(s)	

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Déni de service.

2 Systèmes affectés

Les versions suivantes de Solaris (plates-formes SPARC et x86) sont vulnérables :

- Solaris 7 ;
- Solaris 8 ;
- Solaris 9.

3 Résumé

Selon Sun, deux vulnérabilités présentes dans son système d'exploitation Solaris permettent à un utilisateur mal intentionné d'effectuer un déni de service sur le système vulnérable.

4 Description

- Une vulnérabilité découverte dans le serveur `FTP` (File Transport Protocol) permet à un individu malveillant d'effectuer un déni de service à distance, en consommant l'ensemble des ports disponible sur le système vulnérable au moyen de l'envoi de nombreuses commandes `PASV` (CAN-1999-0079) ;
- la seconde vulnérabilité est causée par une erreur dans la gestion des paquets `ARP` (Address Resolution Protocol). Elle permet à une personne mal intentionnée présente sur le réseau local, d'effectuer un déni de service en innondant le système vulnérable de requêtes `ARP`.

5 Solution

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

6 Documentation

- Bulletin de sécurité #57725 du 14 février 2005 de Sun :
  http://sunsolve.sun.com/search/document.do?assetkey=1-26-57725-1
- Bulletin de sécurité #57673 du 14 février 2005 de Sun :
  http://sunsolve.sun.com/search/document.do?assetkey=1-26-57673-1
- Référence CVE CAN-1999-0079 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0079

Gestion détaillée du document

16 février 2005 version initiale.