



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 3 août 2006
N° CERTA-2006-AVI-325

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la pile IP 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-2006-AVI-325>

Gestion du document

Référence	CERTA-2006-AVI-325
Titre	Vulnérabilité dans la pile IP de Sun Solaris
Date de la première version	3 août 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Sun #102509
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.

3 Résumé

Une vulnérabilité dans la pile IP de Sun Solaris 10 permet à un utilisateur local de contourner la politique de sécurité du système.

4 Description

Une erreur dans la mise en œuvre du protocole IP par le système d'exploitation Sun Solaris 10 autorise le contournement des règles mises en place dans la table de routage afin d'envoyer des paquets vers d'autres destinations que celle déjà définies. Ceci permet à un utilisateur local non-privilegié d'accéder à des services non-accessibles en temps normal ou bien encore de contourner un éventuel pare-feu.

5 Solution

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

6 Documentation

- Bulletin de sécurité Sun Solaris #102509 du 21 juillet 2006 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102509-1>
- Référence CVE CVE-2006-3825 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3825>

Gestion détaillée du document

3 août 2006 version initiale.