

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Déni de service 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-2003-AVI-027>

Gestion du document

Référence	CERTA-2003-AVI-027
Titre	Déni de service sous Solaris
Date de la première version	20 février 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité #50240 de Sun Bulletin de sécurité #50626 de Sun
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

Déni de service.

2 Systèmes affectés

Solaris versions 2.6 à 9.

3 Résumé

Deux bulletins de sécurité décrivant des vulnérabilités permettant à un utilisateur mal intentionné de réaliser un déni de service ont été publiés par Sun.

4 Description

– Le bulletin de sécurité #50240 décrit une vulnérabilité présente dans le serveur `in.ftpd`.

Un utilisateur mal intentionné connecté à un serveur FTP vulnérable peut réaliser un déni de service ("gel" du serveur) empêchant celui-ci de répondre aux requêtes des autres clients. Il est à noter que les clients FTP utilisant le mode `passive` ne sont pas affectés par ce déni de service.

- Une vulnérabilité présente dans le traitement de certains paquets RPC (UDP) entraîne une utilisation excessive de la mémoire.
Cette vulnérabilité permet à un utilisateur mal intentionné de réaliser un déni de service du système vulnérable. Le bulletin de sécurité #50626 décrit les symptômes d'une telle attaque.

5 Solution

Appliquer les correctifs de l'éditeur (se référer à la section Documentation).

6 Documentation

- Bulletin de sécurité #50240 de Sun "Solaris FTP Server is vulnerable to denial of service attack" :
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50240>
- Bulletin de sécurité #50626 de Sun "Certain UDP RPC packet may cause a denial of service in Solaris" :
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50626>

Gestion détaillée du document

20 février 2003 version initiale.