



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 novembre 2008
N° CERTA-2008-AVI-552

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités du serveur DHCP 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-2008-AVI-552>

Gestion du document

Référence	CERTA-2008-AVI-552
Titre	Multiples vulnérabilités du serveur DHCP de Sun Solaris
Date de la première version	13 novembre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Sun #243806 du 07 novembre 2008
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 à distance ;
- déni de service à distance.

2 Systèmes affectés

- Solaris 8 ;
- Solaris 9 ;
- Solaris 10.

3 Résumé

Plusieurs vulnérabilités présentes dans le serveur DHCP de Sun Solaris permettent à un utilisateur distant malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

Deux vulnérabilités sont présentes dans le service `in.dhcpd` de Sun Solaris. La première est de type débordement de mémoire quant à la seconde, elle n'est pas détaillée par l'éditeur.

Toutes deux permettent à un utilisateur distant malintentionné de provoquer un déni de service ou, potentiellement, d'exécuter du code arbitraire.

Compte tenu de la nature du protocole DHCP, l'attaquant devra, sans doute, se situer sur le même sous-réseau que la machine vulnérable pour réaliser l'exploitation.

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 #243806 du 07 novembre 2008 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-243806-1>
- Référence CVE CVE-2007-5365 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5365>

Gestion détaillée du document

13 novembre 2008 version initiale.