

Affaire suivie par :  
CERTA

## AVIS DU CERTA

**Objet : Vulnérabilité de Sun ONE / iPlanet Web Server sous Solaris (iPlanet Admin)**

---

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-2002-AVI-270>

---

### Gestion du document

Référence	CERTA-2002-AVI-270-001
Titre	Vulnérabilité de Sun ONE / iPlanet Web Server sous Solaris (iPlanet Admin)
Date de la première version	18 décembre 2002
Date de la dernière version	10 janvier 2003
Source(s)	Bulletin d'alerte de #49475 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

Exécution de code arbitraire avec les permissions de l'administrateur `root`.

## 2 Systèmes affectés

- Sun ONE / iPlanet Web Server 4.1 Service Pack 1 et toutes les versions précédentes.
- Sun ONE / iPlanet Web Server 6.0 avec ou sans Service Pack 1
- iPlanet Web Server 4.0 avec ou sans Service Pack.
- Netscape Enterprise Server 3.x avec ou sans Service Pack.

## 3 Résumé

Il est possible d'amener l'administrateur du serveur Sun ONE Web Server à exécuter du code arbitraire par le biais de la console d'administration `iPlanet Admin`

## 4 Description

Un utilisateur mal intentionné peut, par le biais d'un script injecté dans les fichiers journaux de Sun ONE Web Server, amener l'administrateur observant ces journaux au moyen de la console `iPlanet Admin` à exécuter du code arbitraire sur le serveur Sun ONE Web Server.

Deux vulnérabilités sont exploitées :

- une vulnérabilité dite de « *Cross Site Scripting* » (XSS) à travers les fichiers journaux ;
- une vulnérabilité de la fonction `Open()` permettant l'exécution de code arbitraire sous Sun ONE Web Server.

## 5 Contournement provisoire

Eviter d'utiliser la console `iPlanet Admin` pour observer les fichiers journaux.

## 6 Solution

Consulter le bulletin d'alerte #49475 de Sun (voir le paragraphe Documentation) pour connaître la disponibilité des correctifs.

## 7 Documentation

- Bulletin d'alerte #49475 de Sun :  
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F49475>
- Bulletin de sécurité #2002-4 de NGSoftware :  
<http://www.ngsec.com/docs/advisories/NGSEC-2002-4.txt>

## Gestion détaillée du document

**18 décembre 2002** version initiale.

**10 janvier 2003** seconde version : modification des systèmes affectés et du paragraphe solution.