Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 juillet 2002
N° CERTA-2002-AVI-146

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnerabilite sur IPlanet

Gestion du document

Référence	CERTA-2002-AVI-146
Titre	Vulnérabilités sur iPlanet Webserver
Date de la première version	11 juillet 2002
Date de la dernière version	–
Source(s)	Avis de sécurité NGSSoftware
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

- Divulgation de données ;
- exécution de code arbitraire.

2 Systèmes affectés

- `iPlanet WebServer 6.0 SP2;`
- `iPlanet WebServer 4.1 SP9;`
- `Netscape Enterprise Server 3.6.`

3 Résumé

Deux vulnérabilités présentes sur `iPlanet Webserver`, dont une sur `Netscape Enterprise`, permettent à un utilisateur mal intentionné d'accéder à des données protégées du système ou d'exécuter du code arbitraire avec les privilèges de l'utilisateur exécutant l'application.

4 Description

Une vulnérabilité sur la fonction de recherche `iPlanet Search` (inactive par défaut) permet à un utilisateur mal intentionné d'exécuter du code arbitraire avec les privilèges de l'utilisateur propriétaire du processus. Cette vulnérabilité, qui ne concerne pas Netscape Entreprise Server, est exploitable à distance par l'envoi de données trop importante à la variable `NS-rel-doc-name`.

Une seconde vulnérabilité sur la variable `NS-query-pat` permet à un utilisateur mal intentionné, par le biais de requêtes spécifiques, d'accéder à des informations protégées du système.

5 Contournement provisoire

Désactiver la fonction de recherche `iPlanet Search`.

6 Solution

Installer le correctif correspondant à votre serveur web (cf section documentation).

7 Documentation

- iPlanet Webserver 6.0 SP3 disponible sur
  http://docs.iplanet.com/docs/manuals/enterprise/60sp3/rn60sp3.html
- iPlanet Webserver 4.1 SP10 disponible sur
  http://docs.iplanet.com/docs/manuals/enterprise/41/rn41sp10.html
- Avis de sécurité NGSSoftware
  http://www.ngssoftware.com/advisories/sun-iws.txt
- Correctif disponible sur le site de sun à l'adresse
  http://wwws.sun.com/software/download/inter_econ.html#webs

Gestion détaillée du document

11 juillet 2002 version initiale.