Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 août 2002
N° CERTA-2002-AVI-172

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités sur les serveurs Web SunONE, iPlanet et Netscape

Gestion du document

Référence	CERTA-2002-AVI-172
Titre	Multiples vulnérabilités sur les serveurs Web SunONE, iPlanet et Netscape
Date de la première version	09 août 2002
Date de la dernière version	–
Source(s)	Avis 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 ;
- déni de service ;
- divulgation de données.

2 Systèmes affectés

Les serveurs Web `SunONE`, `iPlanet` et `Netscape` de versions antérieures à 4.1 SP11 et 6.0 SP4.

3 Résumé

Deux nouvelles vulnérabilités affectent les serveurs Web de Sun. La première est de type débordement de mémoire et permet à un utilisateur mal intentionné d'exécuter un code arbitraire sur le serveur. La deuxième donne accès à des fichiers non autorisés.

4 Description

La première vulnérabilité est présente dans la fonction `Transfer Encoding` du serveur. Une requête malicieusement construite, utilisant la méthode de transfert "`chunked encoding`", reçue par le serveur peut causer un débordement de mémoire. Ce débordement de mémoire peut aboutir à l'exécution de code arbitraire sur le serveur avec les privilèges de l'application.
La deuxième vulnérabilité concerne la commande `NS-query-pat`. Cette commande permet de spécifier le chemin d'un fichier utilisé pour définir le type de la recherche sur un site Web. Le moteur de recherche ne vérifie pas le chemin de ce fichier permettant ainsi le rapatriement de données non autorisées.

5 Contournement provisoire

Si vous ne pouvez pas mettre à jour votre serveur, un module `NSAPI` est disponible sur le site de Sun pour vous permettre de bloquer les accès de type "chunk encoding".
Pour la deuxième vulnérabilité, il est conseillé de désactiver la fonction de recherche sur le serveur. Dans la mesure du possible, il faut restreindre les permissions de l'utilisateur exécutant le serveur Web au minimum. C'est difficile sur les plateformes Windows NT car le serveur fonctionne typiquement avec les permissions d'un service système. Sur les serveurs UNIX, il est conseillé de créer un environnement d'exécution restreint (chroot) pour l'application.

6 Solution

Des correctifs sont disponibles en téléchargement sur le site de Sun, consultez la section Documentation.

7 Documentation

Bulletin de Sun concernant la première vulnérabilité :
http://www.sun.com/service/support/software/iplanet/alerts/transferencodingalert-23july2002.html

Bulletin de Sun concernant la deuxième vulnérabilité :
http://www.sun.com/service/support/software/iplanet/alerts/remotefileviewing-23july2002.html

Page de téléchargement des correctifs :
http://wwws.sun.com/software/download/allproducts.html

Gestion détaillée du document

09 août 2002 version initiale.