Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 septembre 2004
N° CERTA-2004-AVI-278-004

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de la bibliothèque NSS

Gestion du document

Référence	CERTA-2004-AVI-278-004
Titre	Vulnérabilité de la bibliothèque NSS
Date de la première version	26 août 2004
Date de la dernière version	21 septembre 2004
Source(s)	Avis de sécurité ISS du 23 août 2004
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.

2 Systèmes affectés

Tous les produits utilisant la bibliothèque NSS.

3 Résumé

Une vulnérabilité de la bibliothèque NSS permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire sur un système vulnérable.

4 Description

NSS (Network Security Services) est une bibliothèque utilisée pour mettre en oeuvre les communications SSL (Secure Socket Layer).

Elle est principalement utilisée par les serveurs suivants :
– Netscape Enterprise Server ;

- Netscape Personalization Engine ;
- Netscape Directory Server ;
- Netscape Certificate Management Server ;
- Sun One/iPlanet ;
- Sun Java System Web Server.

Une vulnérabilité de type débordement de mémoire a été découverte dans la gestion de la négociation des communications SSlv2 par la bibliothèque NSS.

Cette vulnérabilité permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur le serveur vulnérable. L'attaquant obtiendra les privilèges de l'application utilisant la bibliothèque NSS.

5 Contournement provisoire

Désactiver le support SSLv2.

6 Solution

La version 3.9.2 de NSS corrige cette vulnérabilité. Elle est disponible à l'adresse suivante :
ftp://ftp.mozilla.org/pub/mozilla.org/security/nss/releases/NSS_3_9_2_RTM/

7 Documentation

- Avis de sécurité ISS du 23 août 2004 :
  http://xforce.iss.net/xforce/alerts/id/180
- Bulletin de sécurité FreeBSD pour nss du 27 août 2004 :
  http://www.vuxml.org/freebsd/
- Bulletin de sécurité de Sun du 30 août 2004 :
  http://sunsolve.sun.com/search/document.do?assetkey=1-26-57632-1
- Bulletin de sécurité de Sun du 16 septembre 2004 :
  http://sunsolve.sun.com/search/document.do?assetkey=1-26-57643-1
- Bulletin de sécurité HPSBUX01070 du 23 août 2004 pour HP-UX :
  http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01070
- Référence CVE CAN-2004-0826 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0826

Gestion détaillée du document

26 août 2004 version initiale.
30 août 2004 ajout de la référence au bulletin de sécurité FreeBSD.
01 septembre 2004 ajout de la référence au bulletin de sécurité Sun.
08 septembre 2004 ajout de la référence au bulletin de sécurité HP et ajout de la référence CVE.
21 septembre 2004 ajout de la référence au bulletin de sécurité de SUN du 16 septembre 2004.