Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 mars 2002
N° CERTA-2000-AVI-079

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Netscape sous Unix

Gestion du document

Référence	CERTA-2000-AVI-079
Titre	Vulnérabilité de Netscape sous Unix
Date de la première version	01 décembre 2000
Date de la dernière version	28 mars 2002
Source(s)	Bulletin de sécurité RedHat Avis de sécurité FreeBSD
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

- Déni de service,
- exécution de code arbitraire.

2 Systèmes affectés

La vulnérabilité concerne des clients Netscape de version inférieure ou égale à 4.75, elle est connue sous FreeBSD et RedHat Linux mais peut exister sous d'autres systèmes (toute distribution Linux en particulier).

3 Résumé

Un débordement de mémoire permet à l'administrateur d'un site malicieux d'arrêter à distance un client Netscape ou d'exécuter du code arbitraire sur la machine du client qui le visite.

4 Description

Une vulnérabilité de l'analyseur syntaxique HTML de Netscape versions 4.75 et inférieures, permet à un utilisateur mal intentionné d'arrêter le client qui visiterait son site, voire même, de lui faire exécuter du code arbitraire, en amenant sa victime à visiter une page web habilement conçue.

5 Solution

- Pour Red Hat Linux, installer la version 4.76 de Netscape.
  - 6.0 sur i386:
    ftp://updates.redhat.com/6.0/i386/netscape-common-4.76-0.6.2.i386.rpm
    ftp://updates.redhat.com/6.0/i386/netscape-communicator-4.76-0.6.2.i386.rpm
    ftp://updates.redhat.com/6.0/i386/netscape-navigator-4.76-0.6.2.i386.rpm
    Sources:
    ftp://updates.redhat.com/6.0/SRPMS/netscape-4.76-0.6.2.src.rpm
  - 6.1 sur i386:
    ftp://updates.redhat.com/6.1/i386/netscape-common-4.76-0.6.2.i386.rpm
    ftp://updates.redhat.com/6.1/i386/netscape-communicator-4.76-0.6.2.i386.rpm
    ftp://updates.redhat.com/6.1/i386/netscape-navigator-4.76-0.6.2.i386.rpm
    Sources:
    ftp://updates.redhat.com/6.1/SRPMS/netscape-4.76-0.6.2.src.rpm
  - 6.2 pour alpha :
    ftp://updates.redhat.com/6.2/alpha/netscape-common-4.76-0.6.2.alpha.rpm
    ftp://updates.redhat.com/6.2/alpha/netscape-communicator-4.76-0.6.2.alpha.rpm
    ftp://updates.redhat.com/6.2/alpha/netscape-navigator-4.76-0.6.2.alpha.rpm
  - 6.2 pour i386:
    ftp://updates.redhat.com/6.2/i386/netscape-common-4.76-0.6.2.i386.rpm
    ftp://updates.redhat.com/6.2/i386/netscape-communicator-4.76-0.6.2.i386.rpm
    ftp://updates.redhat.com/6.2/i386/netscape-navigator-4.76-0.6.2.i386.rpm
    Sources:
    ftp://updates.redhat.com/6.2/SRPMS/netscape-alpha-4.76-0.6.2.src.rpm
    ftp://updates.redhat.com/6.2/SRPMS/netscape-4.76-0.6.2.src.rpm
  - 7.0 pour alpha :
    ftp://updates.redhat.com/7.0/alpha/netscape-common-4.76-1.alpha.rpm
    ftp://updates.redhat.com/7.0/alpha/netscape-communicator-4.76-1.alpha.rpm
    ftp://updates.redhat.com/7.0/alpha/netscape-navigator-4.76-1.alpha.rpm
  - 7.0 pour i386:
    ftp://updates.redhat.com/7.0/i386/netscape-common-4.76-1.i386.rpm
    ftp://updates.redhat.com/7.0/i386/netscape-communicator-4.76-1.i386.rpm
    ftp://updates.redhat.com/7.0/i386/netscape-navigator-4.76-1.i386.rpm
    Sources:
    ftp://updates.redhat.com/7.0/SRPMS/netscape-alpha-4.76-1.src.rpm
    ftp://updates.redhat.com/7.0/SRPMS/netscape-4.76-1.src.rpm
- Pour FreeBSD, après avoir supprimé le module de portage, installer le correctif selon le numéro de version de FreeBSD (3 pour la version 3.5, 4 pour 4.2 ou 5 pour 5.0) :
  - Pour i386 (selon la version) :
    ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-3-stable/www/
    ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-4-stable/www/
    ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-5-current/www/
  - Pour alpha (selon la version):
    ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-4-stable/www/
    ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-5-stable/www/

6 Documentation

- L'avis de sécurité de RedHat :
  http://www.redhat.com/support/errata/RHSA-2000-109.html
- L'avis de sécurité FreeBSD :
  ftp://ftp.freebsd.org/pub/FreeBSD/advisories/FreeBSD-SA-00:66.netscape.asc

Gestion détaillée du document

01 décembre 2000 version initiale.
28 mars 2002 première révision : correction d'un lien.