



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 juillet 2000
N° CERTA-2000-AVI-018

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sous Netscape 4.73 et antérieures

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-2000-AVI-018>

Gestion du document

Référence	CERTA-2000-AVI-018
Titre	Vulnérabilité sous Netscape 4.73 et antérieures
Date de la première version	27 juillet 2000
Date de la dernière version	–
Source(s)	Security Focus
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

- Dénier de service ;
- Exécution de code arbitraire.

2 Systèmes affectés

- Netscape 4.73 et antérieures ;
- Mozilla M15.

3 Résumé

Certaines versions de Netscape sont vulnérables lors de l'affichage d'images jpg mal formées, durant la consultation d'un site, la lecture d'un mël ou d'un groupe de discussion. Au mieux Netscape « plante », au pire il exécute du code malveillant.

4 Description

JPEG est un format d'image compressée très populaire sur internet. Dans le format JPEG les en-têtes sont constituées de plusieurs champs d'information. Un utilisateur malveillant peut construire une image ne respectant pas la structure de ces champs. Lorsque Netscape charge une telle image, celle-ci exploite alors le débordement d'une variable pour le faire « planter » ou bien lui faire exécuter du code.

Comme tous les sites webs contiennent des images, le simple fait de naviguer s'avère dès lors très dangereux. On trouve actuellement des images faisant « planter » Netscape.

5 Solution

Mettre à jour Netscape avec la version 4.74

<http://www.netscape.com/computing/download/index.html>

6 Documentation

Aucune documentation actuellement disponible.

Gestion détaillée du document

27 juillet 2000 version initiale.