Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 juillet 2001
N° CERTA-2001-AVI-077

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans xloadimage

Gestion du document

Référence	CERTA-2001-AVI-077
Titre	Vulnérabilité dans xloadimage
Date de la première version	13 juillet 2001
Date de la dernière version	–
Source(s)	Avis de sécurité RHSA-2001:088-04 de RedHat
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 en local;
- Exécution de code arbitraire à distance (utilisation avec Netscape Navigator).

2 Systèmes affectés

Versions 4.1 et antérieures.
Xloadimage est une application X11 tournant sur de nombreuses plateformes Unix.

3 Résumé

Xloadimage est un outil permettant de visualiser des images de différents formats (GIF, TIFF, JPEG...).
Une vulnérabilité de type débordement de mémoire dans la commande xloadimage permet l'exécution de code arbitraire avec les privilèges de l'utilisateur. Si xloadimage est utilisé avec Netscape, l'exploitation de cette vulnérabilité peut se faire à distance.

4 Description

Une vulnérabilité dans une des routines de chargement d'images peut entrainer sous certaines conditions l'éxecution d'un code arbitraire contenu dans cette image.

Xloadimage est aussi utilisé par Netscape Navigator sur les plateformes Linux pour visualiser des images au format Tiff et SUN Raster. Un utilisateur mal intentionné peut mettre à disposition sur un site Web des images contenant du code arbitraire qui sera exécuté avec les privilèges de l'utilisateur.

5 Contournement provisoire

Paramétrer Netscape Navigator pour empêcher l'utilisation de xloadimage: se référer au fichier de configuration `/etc/pluggerrc` de Netscape Navigator.

6 Solution

Un correctif est disponible sur le site de RedHat :

– ftp://updates.redhat.com/7.0/en/os/SRPMS/xloadimage-4.1-20.src.rpm

Pour les autres distributions, consulter l'éditeur pour les mises-à-jour.

7 Documentation

Avis de sécurité RHSA-2001:088-04 de RedHat

Gestion détaillée du document

13 juillet 2001 version initiale.