

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de xli

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-2005-AVI-392>

Gestion du document

Référence	CERTA-2005-AVI-392-001
Titre	Vulnérabilité de xli
Date de la première version	11 octobre 2005
Date de la dernière version	12 octobre 2005
Source(s)	Bulletin de sécurité Debian DSA-859 du 10 octobre 2005
Pièce(s) jointe(s)	

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Exécution de code arbitraire à distance.

2 Systèmes affectés

- xli 1.x ;
- xloadimage 4.x.

3 Résumé

Une vulnérabilité dans l'application `xloadimage`, également inclu dans `xli`, permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

`xloadimage` et `xli` sont des applications qui permettent de visualiser des images sous le serveur graphique X11.

Une vulnérabilité de type débordement de la pile mémoire, dans les applications `xloadimage` et `xli`, est causée par une erreur dans la gestion des titres d'un fichier image `.NIFF`. Cette vulnérabilité peut être exploitée par un utilisateur distant mal intentionné, via une image au format `.NIFF` habilement constituée, afin d'exécuter du code arbitraire.

5 Solution

Se référer aux bulletins de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Debian DSA-858 du 10 octobre 2005 :
<http://www.debian.org/security/2005/dsa-858>
- Bulletin de sécurité Debian DSA-859 du 10 octobre 2005 :
<http://www.debian.org/security/2005/dsa-859>
- Mise à jour de sécurité Fedora Core 3 pour `xloadimage` :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/>
- Référence CVE CAN-2005-3178 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3178>

Gestion détaillée du document

11 octobre 2005 version initiale.

12 octobre 2005 ajout de la référence au bulletin de sécurité Debian DSA-858.