

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de xloadimage et 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-114>

Gestion du document

Référence	CERTA-2005-AVI-114-004
Titre	Multiples vulnérabilités de xli
Date de la première version	14 mars 2005
Date de la dernière version	17 juin 2005
Source(s)	Bulletin de sécurité Gentoo GLSA 200503-05 du 02 mars 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 ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Toutes les versions antérieures à xli 1.17.0-r1 ;
- toutes les versions antérieures à xloadimage 4.1-r2.

3 Résumé

De multiples vulnérabilités découvertes dans xli permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

xli et xloadimage sont utilisés pour afficher et manipuler un grand choix de formats d'image.

- Une première vulnérabilité découverte dans le traitement des images compressées peut être exploitée par un utilisateur distant mal intentionné afin d’injecter des commandes `shell` au moyen d’un fichier malicieusement nommé ;
- une seconde vulnérabilité de type débordement de mémoire est présente dans la fonction `facesload()`. Cette vulnérabilité permet à un utilisateur mal intentionné d’exécuter du code arbitraire à distance au moyen d’un fichier image malicieusement construit ;
- la validation des propriétés des images présente certaines erreurs pouvant être exploitées afin d’exécuter du code arbitraire.

5 Solution

Se référer au bulletin de sécurité de l’éditeur pour l’obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Gentoo GLSA 200503-05 du 02 mars 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200503-05.xml>
- Bulletin de sécurité Debian DSA-694 du 21 mars 2005 :
<http://www.debian.org/security/2005/dsa-694>
- Bulletin de sécurité Debian DSA-695 du 21 mars 2005 :
<http://www.debian.org/security/2005/dsa-695>
- Bulletin de sécurité Red Hat RHSA-2005:332 du 19 avril 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-332.html>
- Bulletin de sécurité Mandriva MDKSA-2005:076 du 20 avril 2005 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:076>
- Bulletin de sécurité Avaya ASA-2005-134 du 14 juin 2005 :
http://support.avaya.com/elmodocs2/security/ASA-2005-134_RHSA-2005-332.pdf
- Bulletins de sécurité FreeBSD pour xli et xloadimage du 03 juin 2005 :
<http://www.vuxml.org/freebsd/pkg-xli.html>
<http://www.vuxml.org/freebsd/pkg-xloadimage.html>
- Référence CVE CAN-2001-0775 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0775>
- Référence CVE CAN-2005-0638 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0638>
- Référence CVE CAN-2005-0639 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0639>

Gestion détaillée du document

14 mars 2005 version initiale.

24 mars 2005 changement titre. Ajout référence CVE CAN-2005-0638. Ajout référence aux bulletins de sécurité DSA-694 et DSA-695 de Debian.

21 avril 2005 ajout des références aux bulletins de sécurité Red Hat et Mandriva.

10 juin 2005 ajout des références aux bulletins de sécurité FreeBSD.

17 juin 2005 ajout du bulletin de sécurité Avaya ASA-2005-134.