

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de libXpm

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-104>

Gestion du document

Référence	CERTA-2005-AVI-104-009
Titre	Vulnérabilité de libXpm
Date de la première version	11 mars 2005
Date de la dernière version	09 juin 2005
Source(s)	Bulletin de sécurité Gentoo GLSA 200503-08 du 04 mars 2005
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 à distance.

2 Systèmes affectés

Toutes les versions de libXpm.
LessTif et OpenMotif sont aussi affectés dans la mesure où ils utilisent la bibliothèque libXpm.

3 Résumé

Un débordement de mémoire présent dans la bibliothèque libXpm permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.
Toutes les applications utilisant la bibliothèque libXpm sont potentiellement affectées.

4 Description

libXpm est une bibliothèque pour le traitement des images au format XPM (X Pixmap).
LessTif est un clone de Motif, une boîte à outils standard pour la création d'interface, disponible sous GNU/Linux

et UNIX.

OpenMotif est une version libre de la boîte à outils Motif.

Un débordement de mémoire présent dans le code source `scan.c` de la bibliothèque `libXpm` permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance, via un fichier judicieusement constitué.

Toutes les applications utilisant la bibliothèque `libXpm` sont potentiellement affectées, telles `LessTif` et `OpenMotif`.

5 Solution

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

6 Documentation

- Site Internet de `LessTif` :
<http://www.lesstif.org>
- Site Internet de `OpenMotif` :
<http://www.opengroup.org/openmotif/>
- Bulletin de sécurité Gentoo GLSA 200503-08 du 04 mars 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200503-08.xml>
- Bulletin de sécurité Gentoo GLSA 200503-15 du 12 mars 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200503-15.xml>
- Bulletin de sécurité RedHat RHSA-2005:331-06 du 30 mars 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-331.html>
- Bulletin de sécurité SuSE SUSE-SR:2005:010 du 08 avril 2005 :
http://www.novell.com/linux/security/advisories/2005_10_sr.html
- Mise à jour de sécurité pour Fedora Core 2 du 30 mars 2005 :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/>
- Mise à jour de sécurité pour Fedora Core 3 du 30 mars 2005 :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/>
- Bulletin de sécurité Mandriva MDKSA-2005:080 du 28 avril 2005 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:080>
- Bulletin de sécurité Mandriva MDKSA-2005:081 du 05 mai 2005 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:081>
- Bulletin de sécurité Debian DSA-723 du 09 mai 2005 :
<http://www.debian.org/security/2005/dsa-723>
- Bulletin de sécurité Red Hat RHSA-2005:412 du 11 mai 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-412.html>
- Bulletin de sécurité Red Hat RHSA-2005:473 du 24 mai 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-473.html>
- Bulletin de sécurité Red Hat RHSA-2005:198 du 08 juin 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-198.html>
- Mise à jour de sécurité des paquetages NetBSD `xpm`, `lesstif` et `openmotif` :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/graphics/xpm/README.html>
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/x11/lesstif/README.html>
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/x11/openmotif/README.html>
- Référence CVE CAN-2005-0605 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0605>

Gestion détaillée du document

11 mars 2005 version initiale.

17 mars 2005 ajout référence au bulletin de sécurité Gentoo GLSA 200503-15.

30 mars 2005 ajout références aux mises à jour de sécurité pour Fedora.

31 mars 2005 ajout références aux mises à jour de sécurité pour RedHat.

- 13 avril 2005** ajout référence au bulletin de sécurité SuSE SUSE-SR:2005:010.
- 02 mai 2005** ajout référence au bulletin de sécurité Mandriva.
- 10 mai 2005** ajout références aux bulletins de sécurité Mandriva et Debian relatifs à XFree86.
- 13 mai 2005** ajout référence au bulletin de sécurité Red Hat relatif à openmotif.
- 27 mai 2005** ajout référence au bulletin de sécurité Red Hat (RHSA-2005:473) relatif à lesstif.
- 09 juin 2005** ajout référence au bulletin de sécurité Red Hat (RHSA-2005:198) relatif à xorg-x11.