

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de XFree86, libXpm, LessTif, Motif et OpenMotif

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-2004-AVI-325>

Gestion du document

Référence	CERTA-2004-AVI-325-009
Titre	Vulnérabilités de XFree86, libXpm, LessTif, Motif et OpenMotif
Date de la première version	21 septembre 2004
Date de la dernière version	06 décembre 2004
Source(s)	Bulletin de sécurité SuSE SUSE-SA:2004034 du 17 septembre 2004
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 ;
- déni de service.

2 Systèmes affectés

- XFree86 versions 4.4.99.13 et antérieures.
- Motif 1.2.5.

3 Résumé

Plusieurs vulnérabilités ont été découvertes dans le code de XFree86, libXpm et LessTif.

4 Description

XFree86 est une mise en oeuvre du système X Window très utilisée sur les plates-formes Linux.

LessTif et libXpm sont deux bibliothèques graphiques.

Motif et OpenMotif réutilisant du code de libXpm sont également vulnérables.

Plusieurs vulnérabilités ont été découvertes dans XFree86 concernant la gestion des fichiers image XPM. Elles sont également présentes dans le code des bibliothèques libXpm et LessTif.

- Plusieurs vulnérabilités de type débordement de mémoire permettent à un utilisateur mal intentionné d'exécuter du code arbitraire sur la machine (CVE CAN-2004-0687).
- Une vulnérabilité de type débordement de mémoire permet à un utilisateur mal intentionné de provoquer un déni de service (CVE CAN-2004-0688).

5 Solution

La version 4.4.99.14 de Xfree86 corrige ces vulnérabilités.

La version 1.2.6 de Motif corrige ces vulnérabilités.

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

6 Documentation

- Site internet de XFree86 :
<http://www.xfree.org>
- Bulletin de sécurité Mandrake MDKSA-2004:098 du 15 septembre 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:098>
- Bulletin de sécurité Mandrake MDKSA-2004:099 du 15 septembre 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:099>
- Bulletin de sécurité SuSE SUSE-SA:2004034 du 17 septembre 2004 :
http://www.suse.com/de/security/2004_34_xfree86_libs_xshared.html
- Bulletin de sécurité FreeBSD pour xpm du 15 septembre 2004 :
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité Gentoo GLSA 200409-34 du 27 septembre 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200409-34.xml>
- Bulletin de sécurité Gentoo GLSA 200410-09 du 09 octobre 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200410-09.xml>
- Bulletin de sécurité Red Hat RHSA-2004:478 du 04 octobre 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-478.html>
- Bulletin de sécurité Red Hat RHSA-2004:537 du 02 décembre 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-537.html>
- Bulletin de sécurité Debian DSA-560 du 07 octobre 2004 :
<http://www.debian.org/security/2004/dsa-560>
- Bulletin de sécurité Debian DSA-561 du 11 octobre 2004 :
<http://www.debian.org/security/2004/dsa-561>
- Bulletin de sécurité Sun #57653 du 08 octobre 2004 :
<http://www.sunsolve.sun.com/search/document.do?assetkey=1-26-57653-1>
- Bulletin de sécurité Sun #57652 du 15 octobre 2004 :
<http://www.sunsolve.sun.com/search/document.do?assetkey=1-26-57652>
- Bulletin de sécurité #19 pour OpenBSD 3.5 du 16 septembre 2004 :
<http://www.openbsd.com/errata#xpm>
- Bulletin de sécurité d'ICS pour Motif :
http://www.ics.com/developers/index.php?cont=xpm_security_alert
- Bulletin de sécurité SSRT4831 pour HP Tru64 Unix du 11 novembre 2004 :
<http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBTU01093>
- Référence CVE CAN-2004-0687 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0687>
- Référence CVE CAN-2004-0688 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0688>

Gestion détaillée du document

21 septembre 2004 version initiale.

27 septembre 2004 ajout du bulletin Gentoo.

08 octobre 2004 LessTif est prise en compte. Ajout de la référence au bulletin de sécurité de Red Hat (RHSA-2004-078) et Debian (DSA-560).

11 octobre 2004 ajout référence au bulletin de sécurité Gentoo GLSA 200410-09 relatif à LessTif.

13 octobre 2004 ajout référence au bulletin de sécurité Debian (DSA-561) et Sun.

15 octobre 2004 ajout référence au bulletin de sécurité OpenBSD.

20 octobre 2004 ajout référence au bulletin de sécurité #57652 de Sun.

21 octobre 2004 Prise en compte de Motif et OpenMotif.

16 novembre 2004 ajout référence au bulletin de sécurité SSRT4831 pour HP Tru64.

06 décembre 2004 ajout référence au bulletin de sécurité Red Hat RHSA-2004:537 relatif à OpenMotif.