Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 décembre 2004
N° CERTA-2004-AVI-376-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de libXpm, XFree86 et X.Org

Gestion du document

Référence	CERTA-2004-AVI-376-002
Titre	Vulnérabilité de libXpm, XFree86 et X.Org
Date de la première version	23 novembre 2004
Date de la dernière version	21 décembre 2004
Source(s)	Bulletin de sécurité SUSE SUSE-SA:2004:041 du 17 novembre 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

- Déni de service ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

Toutes les versions de `libXpm`, `XFree86` et `X.Org`.

3 Résumé

Plusieurs vulnérabilités ont été découvertes dans le code de `libXpm`, `XFree86` et `X.Org` permettant à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

`libXpm` est une bibliothèque graphique de manipulation de fichiers au format XPM (`Pixmap X`).
`libXpm` est notamment utilisée par `XFree86` et `X.Org`.
Lors d'une revue de code, plusieurs vulnérabilités ont été découvertes permettant à un utilisateur mal intentionné,

via un fichier au format XPM habilement constitué, de réaliser un déni de service ou d'exécuter du code arbitraire sur la plate-forme vulnérable.

5 Solution

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
- Site Internet X.Org :
  http://www.x.org
- Bulletin de sécurité SUSE SUSE-SA:2004:041 du 17 novembre 2004 :
  http://www.suse.com/de/security/2004_41_xshared_XFree86_libs_xorg_x11_libs.html
- Bulletin de sécurité Gentoo GLSA 200411-28 du 19 novembre 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200411-28.xml
- Bulletin de sécurité Mandrake MDKSA-2004:137 du 22 novembre 2004 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:137
- Bulletin de sécurité Mandrake MDKSA-2004:138 du 22 novembre 2004 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:138
- Bulletin de sécurité Debian DSA-607 du 10 décembre 2004 :
  http://www.debian.org/security/2004/dsa-607
- Bulletin de sécurité Red Hat RHSA-2004:610 du 20 décembre 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-610.html
- Bulletin de sécurité Red Hat RHSA-2004:612 du 20 décembre 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-612.html
- Référence CVE CAN-2004-0914 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0914

Gestion détaillée du document

23 novembre 2004 version initiale.
16 décembre 2004 ajout référence au bulletin de sécurité de Debian.
21 décembre 2004 ajout référence aux bulletins de sécurité de Red Hat.