Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 décembre 2005
N° CERTA-2005-AVI-461-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des blibliothèques graphiques GTK+2 et Gdk-Pixbuf

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-461

Gestion du document

Référence	CERTA-2005-AVI-461-003
Titre	Vulnérabilité des blibliothèques graphiques GTK+2 et Gdk-Pixbuf
Date de la première version	17 novembre 2005
Date de la dernière version	01 décembre 2005
Source(s)	Bulletin de sécurité iDefense du 15 novembre 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, éventuellement à distance,
- déni de service.

2 Systèmes affectés

Tout système utilisant la boîte à outils graphique `GTK+2` ou la bibliothèque `Gdk-Pixbuf` pour afficher certaines images.

3 Résumé

Un utilisateur mal intentionné peut concevoir un fichier graphique au format `XPM` volontairement mal formé qui provoquera, lors de sa visualisation par une victime, l'exécution de code arbitraire ou un déni de service.

4 Description

`GTK+2` est disponible pour tout système `Unix` utilisant `X Window` mais également pour les systèmes `Microsoft Windows` ou le moteur de rendu graphique `DirectFB` pour `Linux`.

`XPM` est un format d'image utilisé en particulier pour les icônes. Une mauvaise gestion d'une allocation mémoire peut permettre l'exécution de code arbitraire avec les privilèges de l'utilisateur courant. Des navigateurs, clients de messagerie,... utilisant `GTK+2` avec certains systèmes d'exploitation (`Firefox` sous `Linux`, `Sylpheed` sous `Unix` comme `Windows`,...), l'exécution de code à distance est alors possible au moyen de messages, sites web,... malicieux.

5 Solution

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

6 Documentation

- Bulletin de sécurité iDefense du 15 novembre 2005 :
  http://www.idefense.com/application/poi/display?id=339
- Mise à jour de sécurité Fedora Core 3 (gdk-pixbuf et gtk2) du 15 novembre 2005 :
  http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/
- Mise à jour de sécurité Fedora Core 4 du (gdk-pixbuf et gtk2) 15 novembre 2005 :
  http://download.fedora.redhat.com/pub/fedora/linux/core/updates/4/
- Bulletin de sécurité Gentoo GLSA-200511-14 du 16 novembre 2005 :
  http://www.gentoo.org/security/en/glsa/glsa-200511-14.xml
- Bulletin de sécurité RedHat RHSA-2005:810 du 15 novembre 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-810.html
- Bulletin de sécurité RedHat RHSA-2005:811 du 15 novembre 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-811.html
- Bulletin de sécurité SUSE SuSE-SA:2005:065 du 16 novembre 2005 :
  http://www.novell.com/linux/security/advisories/2005_65_gtk2.html
- Bulletin de sécurité Ubuntu USN-216-1 du 16 novembre 2005 :
  http://www.ubuntulinux.org/usn/usn-216-1
- Bulletin de sécurité Gentoo GLSA 200511-14 du 16 novembre 2005 :
  http://www.gentoo.org/security/en/glsa/glsa-200511-14.xml
- Bulletin de sécurité Mandriva MDKSA-2005:214 du 18 novembre 2005 :
  http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:214
- Bulletin de sécurité Debian DSA-911 du 29 novembre 2005 :
  http://www.debian.org/security/2005/dsa-911
- Bulletin de sécurité Debian DSA-913 du 01 décembre 2005 :
  http://www.debian.org/security/2005/dsa-913
- Référence CVE CVE-2005-2975 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2975
- Référence CVE CVE-2005-2976 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2976
- Référence CVE CVE-2005-3186 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3186

Gestion détaillée du document

17 novembre 2005 version initiale.

21 novembre 2005 ajout des références aux bulletins de sécurité Mandriva et Gentoo.

29 novembre 2005 ajout de la référence au bulletin de sécurité Debian DSA-911.

01 décembre 2005 ajout de la référence au bulletin de sécurité Debian DSA-913.