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 juin 2007
N° CERTA-2007-AVI-240

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans GIMP

Gestion du document

Référence	CERTA-2007-AVI-240
Titre	Vulnérabilité dans GIMP
Date de la première version	01 juin 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Ubuntu USN-467-1 du 31 mai 2007
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

GIMP 2.x.

3 Résumé

Une vulnérabilité dans GIMP permet à un utilisateur distant malintentionné d'exécuter du code arbitraire à distance sur le système vulnérable.

4 Description

GIMP (Gnu Image Manipulation Program) est un logiciel libre sous licence GPL de retouche d'images.

Une vulnérabilité de type débordement de pile dans la fonction set_color_table() permet à un utilisateur malveillant d'exécuter du code arbitraire au moyen d'un fichier image, spécialement conçu, au format raster dont l'extension est .ras.

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-200705-08 du 07 mai 2007 :
  http://www.gentoo.org/security/en/glsa/glsa-200705-08.xml
- Bulletin de sécurité Mandriva MDKSA-2007:108 du 22 mai 2007 :
  http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2007:108
- Bulletin de sécurité RedHat RHSA-2007:21 du 21 juin 2007 :
  http://rhn.redhat.com/errata/RHSA-2007-21.html
- Bulletin de sécurité SuSE SUSE-SR:2007:011 du 16 juin 2007 :
  http://lists.suse.com/archive/suse-security-announce/2007-May/0005.html
- Bulletin de sécurité Ubuntu USN-467-1 du 31 mai 2007 :
  http://www.ubuntulinux.org/usn/usn-467-1
- Référence CVE CVE-2007-2356 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2356

Gestion détaillée du document

01 juin 2007 version initiale.