Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 août 2007
N° CERTA-2007-AVI-290-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans GIMP

Gestion du document

Référence	CERTA-2007-AVI-290-002
Titre	Vulnérabilités dans GIMP
Date de la première version	10 juillet 2007
Date de la dernière version	27 août 2007
Source(s)	Mise à jour 2.2.16 de GIMP
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 versions 2.2.15 et antérieures.

3 Résumé

Plusieurs vulnérabilités dans GIMP permettent à une personne d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités de type débordement de mémoire ont été identifiées dans des modules de GIMP. Celles-ci permettent à un attaquant d'exécuter du code arbitraire sur le poste d'un utilisateur qui a ouvert un fichier image spécialement conçu.

5 Solution

La version 2.2.16 de GIMP corrige ces vulnérabilités.

6 Documentation

- Mises à jour de GIMP :
  http://developer.gimp.org/NEWS-2.2
- Bulletin de sécurité Gentoo GLSA-200707-09 du 25 juillet 2007 :
  http://www.gentoo.org/security/en/glsa/glsa-200707-09.xml
- Bulletin de sécurité Debian DSA-1335 18 juillet 2007 :
  http://www.debian.org/security/2007/dsa-1335
- Bulletin de sécurité Mandriva MDKSA-2007:170 du 23 août 2007 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2007:170
- Bulletin de sécurité Ubuntu USN-480-1 04 juillet 2007 :
  http://www.ubuntu.com/usn/usn-480-1
- Bulletin de sécurité Ubuntu USN-494-1 02 août 2007 :
  http://www.ubuntu.com/usn/usn-494-1
- Référence CVE CVE-2006-4519 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4519
- Référence CVE CVE-2007-2949 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2949

Gestion détaillée du document

10 juillet 2007 version initiale.
27 juillet 2007 ajout des références aux bulletins de sécurité Gentoo, Debian et Ubuntu.
27 août 2007 ajout des références aux bulletins de sécurité Mandriva et Ubuntu.