Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 décembre 2009
N° CERTA-2009-AVI-508-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans GIMP

Gestion du document

Référence	CERTA-2009-AVI-508-002
Titre	Multiples vulnérabilités dans GIMP
Date de la première version	20 novembre 2009
Date de la dernière version	08 janvier 2010
Source(s)	Notes de modification du 09 et 17 novembre 2009
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.

2 Systèmes affectés

GIMP 2.6.7 et possiblement les versions antérieures.

3 Résumé

Plusieurs vulnérabilités dans Gimp de type débordement d'entiers permettant au moins un déni de service ont été corrigées.

4 Description

Plusieurs vulnérabilités de type débordement d'entiers, intervenant lors du traitement de fichiers d'image au format `BMP` ou `PSD`, ont été corrigées. Elles permettent à une personne malintentionnée de provoquer un déni de service au moyen d'un fichier spécialement conçu.

5 Solution

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

6 Documentation

- Notes de modification du fichier bmp-read.c du 09 novembre 2009 :
  http://git.gnome.org/cgit/gimp/commit/?id=e3afc99b2fa7aeddf0dba4778663160a5bc682d3
- Note de modification des fichiers psd-load.c et psd.h du 17 novembre 2009 :
  http://git.gnome.org/cgit/gimp/commit/?id=9cc8d78ff33b7a36852b74e64b427489cad44d0e
  http://git.gnome.org/cgit/gimp/commit/?id=0e440cb6d4d6ee029667363d244aff61b154c33c
- Bulletin de sécurité Sun Solaris #274390 du 15 décembre 2009 :
  http://sunsolve.sun.com/search/document.do?assetkey=1-66-274390-1
- Bulletin de sécurité Ubuntu USN-880-1 du 07 janvier 2010 :
  http://www.ubuntu.com/usn/USN-880-1
- Référence CVE CVE-2009-1570 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1570
- Référence CVE CVE-2009-3909 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3909

Gestion détaillée du document

20 novembre 2009 version initiale ;
17 décembre 2009 ajout du bulletin de sécurité Sun Solaris ;
07 janvier 2010 ajout du bulletin de sécurité Ubuntu.