Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 décembre 2004
N° CERTA-2004-AVI-369-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité d'ImageMagick

Gestion du document

Référence	CERTA-2004-AVI-369-002
Titre	Vulnérabilité d'ImageMagick
Date de la première version	19 novembre 2004
Date de la dernière version	09 décembre 2004
Source(s)	Bulletin de sécurité DSA-593 de Debian
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

ImageMagick dont la version est antérieure à la 6.1.x.

3 Description

ImageMagick est un ensemble d'outils destinés au traitement d'images.

Une vulnérabilité de type débordement de mémoire présente dans la routine de traitement des informations EXIF (Exchangeable Image File Format) contenues dans certaines images peut être exploitée par une personne mal intentionnée mettant à disposition de l'utilisateur d'ImageMagick une image habilement constituée.

4 Solution

La version 6.1.x corrige cette vulnérabilité.

5 Documentation

- Site d'ImageMagick :
  http://www.imagemagick.org
- Sortie de la version 6.1 :
  http://sourceforge.net/projects/shownotes.php?release_id=273318
- Bulletin de sécurité Debian DSA-593 du 16 novembre 2004 :
  http://www.debian.org/security/2004/dsa-593
- Bulletin de sécurité Gentoo GLSA 200411-11 du 06 novembre 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200411-11.xml
- 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 Mandrake MDKSA-2004:143 du 6 décembre 2004 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:143
- Bulletin de sécurité RedHat RHSA-2004:636 du 08 décembre 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-636.html
- Référence CVE CAN-2004-0981 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0981

Gestion détaillée du document

19 novembre 2004 version initiale.
07 décembre 2004 ajout de la référence au bulletin de sécurité de Mandrake.
09 décembre 2004 ajout de la référence au bulletin de sécurité de RedHat.