



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 avril 2005
N° CERTA-2005-AVI-122-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans ImageMagick

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-122>

Gestion du document

Référence	CERTA-2005-AVI-122-002
Titre	Multiples vulnérabilités dans ImageMagick
Date de la première version	25 mars 2005
Date de la dernière version	04 avril 2005
Source(s)	Bulletin de sécurité SUSE-SA:2005:017
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 ;
- déni de service.

2 Systèmes affectés

Toutes les versions de ImageMagick antérieures à la version 6.2.

3 Description

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

Plusieurs vulnérabilités présentes dans le traitement des images au format TIFF (CAN-2005-0759 et CAN-2005-0760) ou SGI (CAN-2005-0762) et des informations PSD (CAN-2005-0761) peuvent être exploitées par une personne mal intentionnée en mettant à disposition de l'utilisateur d'ImageMagick une image habilement constituée.

Une vulnérabilité de type chaîne de format est également présente dans la gestion des noms de fichiers image (CAN-2005-0397).

4 Solution

La version 6.2.0-8 corrige ces vulnérabilités.

5 Documentation

- Site Internet d'ImageMagick :
<http://www.imagemagick.org>
- Bulletin de sécurité Gentoo GLSA 200503-11 du 06 mars 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200503-11.xml>
- Bulletin de sécurité RedHat RHSA-2005:070 du 23 mars 2005 :
<https://rhn.redhat.com/errata/RHSA-2005-070.html>
- Bulletin de sécurité RedHat RHSA-2005:320 du 23 mars 2005 :
<https://rhn.redhat.com/errata/RHSA-2005-320.html>
- Mise à jour de sécurité pour Fedora Core 2 du 31 mars 2005 :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/>
- Mise à jour de sécurité pour Fedora Core 3 du 31 mars 2005 :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/>
- Bulletin de sécurité SuSE SuSE-SA:2005:017 du 23 mars 2005 :
http://www.novell.com/linux/security/advisories/2005_17_imagemagick.html
- Bulletin de sécurité Mandrake MDKSA-2005:065 du 01 avril 2005 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:065>
- Bulletin de sécurité Debian DSA-702 du 01 avril 2005 :
<http://www.debian.org/security/2005/dsa-702>
- Bulletin de sécurité FreeBSD pour ImageMagick du 03 mars 2005 :
<http://www.vuxml.org/freebsd/pkg-ImageMagick.html>
- Référence CVE CAN-2005-0397 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0397>
- Référence CVE CAN-2005-0759 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0759>
- Référence CVE CAN-2005-0760 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0760>
- Référence CVE CAN-2005-0761 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0761>
- Référence CVE CAN-2005-0762 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0762>

Gestion détaillée du document

25 mars 2005 version initiale.

31 mars 2005 ajout des références aux mises à jour de sécurité Fedora.

04 avril 2005 ajout des références aux bulletins de sécurité de Mandrake et Debian.