



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 31 mars 2005
N° CERTA-2005-AVI-020-004

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de 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-020>

Gestion du document

Référence	CERTA-2005-AVI-020-004
Titre	Vulnérabilité de ImageMagick
Date de la première version	20 janvier 2005
Date de la dernière version	31 mars 2005
Source(s)	Bulletin de sécurité iDEFENSE 01.17.05
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

Toutes les versions de ImageMagick antérieures à la version 6.1.8-8.

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 PSD (Photoshop Document) 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 6.1.8-8 corrige cette vulnérabilité.

5 Documentation

- Site Internet d'ImageMagick :
<http://www.imagemagick.org>
- Bulletin de sécurité iDEFENSE 01.17.05 du 17 janvier 2005 :
<http://www.odefense.com/application/poi/display?id=184>
- Bulletin de sécurité Debian DSA-646 du 19 janvier 2005 :
<http://www.debian.org/security/2005/dsa-646>
- Bulletin de sécurité Gentoo GLSA 200501-26 du 20 janvier 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200501-26.xml>
- Bulletin de sécurité Gentoo GLSA 200501-37 du 26 janvier 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200501-37.xml>
- Bulletin de sécurité RedHat RHSA-2005:071 du 15 février 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-071.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/>
- Mise à jour de sécurité du paquetage NetBSD ImageMagick :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/graphics/ImageMagick/README.html>
- Référence CVE CAN-2005-0005 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0005>

Gestion détaillée du document

20 janvier 2005 version initiale.

21 janvier 2005 ajout de la référence au bulletin de sécurité Gentoo.

31 janvier 2005 ajout de la référence au second bulletin de sécurité Gentoo et au bulletin de sécurité NetBSD.

17 février 2005 ajout de la référence au bulletin de sécurité RedHat.

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