



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 octobre 2004
N° CERTA-2004-AVI-295-006

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-2004-AVI-295>

Gestion du document

Référence	CERTA-2004-AVI-295-006
Titre	Vulnérabilité dans ImageMagick
Date de la première version	02 septembre 2004
Date de la dernière version	21 octobre 2004
Source(s)	Bulletin de sécurité #1011103 de SecurityTracker
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 6.0.6-2.

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 décodage des fichiers BMP compressés au format RLE 8 bits peut être exploitée par une personne mal intentionnée mettant à disposition de l'utilisateur d'ImageMagick une image habilement constituée.

4 Solution

La version 6.0.6-2 d'ImageMagick corrige cette vulnérabilité.

5 Documentation

- Site Internet d'ImageMagick :
<http://www.imagemagick.org>
- Bulletin de sécurité SecurityTracker #1011103 du 31 août 2004 :
<http://www.securitytracker.com/alerts/2004/Aug/1011103.html>
- Bulletin de sécurité Gentoo GLSA 200409-12 du 08 septembre 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200409-12.xml>
- Bulletin de sécurité Debian DSA-547 du 16 septembre 2004 :
<http://www.debian.org/security/2004/dsa-547>
- Bulletin de sécurité Sun #57648 du 20 septembre 2004 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-57648-1>
- Bulletin de sécurité Mandrake MDKSA-2004:102 du 22 septembre 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:102>
- Bulletin de sécurité Red Hat RHSA-2004:480 du 20 octobre 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-480.html>
- Bulletin de sécurité Red Hat RHSA-2004:494 du 20 octobre 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-494.html>
- Bulletin de sécurité FreeBSD du 31 août 2004 :
<http://www.vuxml.org/freebsd/>
- Mise-à-jour ImageMagick<6.0.6.2 pour NetBSD :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/distfiles/vulnerabilities>

Gestion détaillée du document

02 septembre 2004 version initiale.

08 septembre 2004 ajout de la référence au bulletin de sécurité Gentoo.

17 septembre 2004 ajout de la référence au bulletin de sécurité Debian.

22 septembre 2004 ajout de la référence au bulletin de sécurité Sun.

23 septembre 2004 ajout de la référence au bulletin de sécurité Mandrake.

28 septembre 2004 ajout de la référence au bulletin FreeBSD et à la mise-à-jour NetBSD.

21 octobre 2004 ajout de la référence aux bulletins de sécurité de Red Hat.