



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 février 2008
N° CERTA-2006-AVI-083-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du logiciel 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-2006-AVI-083>

Gestion du document

Référence	CERTA-2006-AVI-083-003
Titre	Vulnérabilité du logiciel ImageMagick
Date de la première version	17 février 2006
Date de la dernière version	06 février 2008
Source(s)	Bulletin de sécurité Gentoo GLSA 200602-06
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 ;
- déni de service à distance.

2 Systèmes affectés

ImageMagick versions inférieures à la version 6.2.5.5.

3 Résumé

Une vulnérabilité présente dans le logiciel ImageMagick permet à un utilisateur mal intentionné de provoquer l'arrêt inopiné du programme ou d'exécuter du code arbitraire à distance.

4 Description

ImageMagick est une suite logicielle permettant de manipuler et gérer des images. Il peut être utilisé comme système de gestion de contenu ou de galeries d'images.

Une vulnérabilité de type *format de chaîne de caractères* a été découverte dans cette suite logicielle. L'exploitation de cette faille permet à un utilisateur mal intentionné de provoquer l'arrêt du logiciel ou d'exécuter du code arbitraire à distance, via un nom de fichier malicieusement construit.

5 Solution

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

6 Documentation

- Bulletin de sécurité Gentoo GLSA-200602-06 du 13 février 2006 :
<http://www.gentoo.org/security/en/glsa/glsa-200602-06.xml>
- Bulletin de sécurité Mandriva MDKSA-2006:024 du 13 février 2006 :
<http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2006:024>
- Bulletin de sécurité RedHat RHSA-2006:0178 du 13 février 2006 :
<http://rhn.redhat.com/errata/RHSA-2006-0178.html>
- Bulletin de sécurité Ubuntu USN-246-1 du 14 février 2006 :
<http://www.ubuntulinux.org/usn/usn-246-1>
- Bulletin de sécurité RedHat RHSA-2006:0178 du 14 février 2006 :
<https://rhn.redhat.com/errata/RHSA-2006-0178.html>
- Bulletin de sécurité Gentoo GLSA-200602-13 du 26 février 2006 :
<http://www.gentoo.org/security/en/glsa/glsa-200602-13.xml>
- Référence CVE CVE-2006-0082 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0082>
- Document de sécurité 231321 publié par Sun Microsystems le 30 janvier 2008 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-231321-1>

Gestion détaillée du document

17 février 2006 version initiale.

27 février 2006 ajout de la référence au bulletin de sécurité RedHat RHSA-2006:0178.

08 mars 2006 ajout de la référence au bulletin de sécurité Gentoo GLSA-200602-13.

06 février 2008 ajout de la référence Sun 231321 concernant Sun Solaris 9 et 10.