



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 septembre 2006
N° CERTA-2006-AVI-361-002

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-2006-AVI-361>

Gestion du document

Référence	CERTA-2006-AVI-361-002
Titre	Vulnérabilité dans ImageMagick
Date de la première version	17 août 2006
Date de la dernière version	28 septembre 2006
Source(s)	Mise à jour de sécurité ImageMagick
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

ImageMagick 6.2.8 et versions antérieures.

3 Description

Une vulnérabilité de type débordement de mémoire a été découverte dans l'application ImageMagick. Elle permet à un utilisateur mal intentionné de provoquer un déni de service au moyen d'une image au format SGI spécialement construite. Cette vulnérabilité pourrait également permettre l'exécution de code arbitraire sur le système vulnérable.

4 Solution

Appliquer la mise à jour de sécurité en passant à la version 6.2.9 de ImageMagick disponible à l'adresse suivante :

<http://www.imagemagick.org/script/download.php>

5 Documentation

- Site Internet de l'éditeur :
<http://www.imagemagick.org>
- Mise à jour de sécurité ImageMagick 6.2.9 :
<http://www.imagemagick.org/script/download.php>
- Bulletin de sécurité Gentoo GLSA-200609-14 du 26 septembre 2006 :
<http://www.gentoo.org/security/en/glsa/glsa-200609-14.xml>
- Bulletin de sécurité RedHat RHSA-2006:0633 du 24 août 2006 :
<http://rhn.redhat.com/errata/RHSA-2006-0633.html>
- Bulletin de sécurité Mandriva MDKSA-2006:155 du 29 août 2006 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2006:155>
- Bulletin de sécurité Debian DSA-1168 du 04 septembre 2006 :
<http://www.debian.org/security/2006/dsa-1168>
- Bulletin de sécurité Ubuntu USN-340-1 du 06 septembre 2006 :
<http://www.ubuntu.com/usn/usn-340-1>
- Bulletin de sécurité SuSE SUSA-SA:2006:050 du 08 septembre 2006 :
http://www.novell.com/linux/security/advisories/2006_50_imagemagick.html
- Référence CVE CVE-2006-3743 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3743>
- Référence CVE CVE-2006-3744 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3744>

Gestion détaillée du document

17 août 2006 version initiale.

11 septembre 2006 ajout des références CVE et des bulletins de sécurité de RedHat, Mandriva, Debian, Ubuntu, SuSE.

28 septembre 2006 ajout de la référence au bulletin de sécurité de Gentoo.