

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Python

---

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-2008-AVI-018>

---

### Gestion du document

Référence	CERTA-2008-AVI-018
Titre	Vulnérabilités dans Python
Date de la première version	15 janvier 2008
Date de la dernière version	–
Source(s)	CVE-2007-4965
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

Applications utilisant le module *imageop* de Python, versions 2.5.1 et précédentes.

## 3 Résumé

Des vulnérabilités dans le module *imageop* de Python permettent à un utilisateur malveillant de provoquer un déni de service ou d'exécuter un code arbitraire à distance.

## 4 Description

Des débordements d'entiers ne sont pas correctement gérés dans le module *imageop* de Python. Un utilisateur malveillant, capable de soumettre une image spécialement conçue à une application utilisant le module vulnérable, peut provoquer un déni de service ou d'exécuter un code arbitraire à distance.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité Apple 307179 du 02 janvier 2008 :  
<http://docs.info.apple.com/article.html?artnum=307179>
- Mise à jour de sécurité Fedora FEDORA-2007-2663 du 29 octobre 2007 :  
<https://www.redhat.com/archives/fedora-package-announcement/2007-October/msg00378.html>
- Bulletin de sécurité Gentoo GLSA-200711-07 du 07 novembre 2007 :  
<http://www.gentoo.org/security/en/glsa/glsa-200711-07.xml>
- Bulletin de sécurité Mandriva MDVSA-2008:013 du 14 janvier 2008 :  
<http://www.mandriva.com/archives/security/advisories>
- Bulletin de sécurité RedHat RHSA-2007:1076 du 10 décembre 2007 :  
<http://rhn.redhat.com/errata/RHSA-2007-1076.html>
- Référence CVE CVE-2007-4965 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4965>

## Gestion détaillée du document

**15 janvier 2008** version initiale.