

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans ClamAV

---

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-012>

---

### Gestion du document

Référence	CERTA-2006-AVI-012-004
Titre	Vulnérabilité dans ClamAV
Date de la première version	10 janvier 2006
Date de la dernière version	08 mars 2006
Source(s)	Site de ClamAV
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

Inconnu.

## 2 Systèmes affectés

ClamAV versions antérieures à 0.88.

## 3 Description

Une vulnérabilité a été découverte dans le fichier `libclamav/upx.c`. Cette vulnérabilité pourrait être exploitée par l'intermédiaire d'un fichier compressé avec UPX malicieusement constitué.

## 4 Solution

Mettre à jour en version 0.88.

## 5 Documentation

- Site Internet de ClamAV :  
<http://www.clamav.net>
- Téléchargement de la version 0.88 de ClamAV :  
<http://www.clamav.net/stable.php>
- Notes concernant la version 0.88 de ClamAV :  
<http://www.clamav.net/doc/0.88/ChangeLog>
- Bulletin de sécurité Gentoo GLSA 200601-07 du 13 janvier 2006 :  
<http://www.gentoo.org/security/en/glsa/glsa-200601-07.xml>
- Mise à jour de sécurité FreeBSD pour clamav et clamav-devel du 10 janvier 2006 :  
<http://www.vuxml.org/freebsd/pkg-clamav.html>  
<http://www.vuxml.org/freebsd/pkg-clamav-devel.html>
- Mise à jour de sécurité OpenBSD pour clamav du 10 janvier 2006 :  
<http://www.vuxml.org/openbsd/pkg-clamav.html>
- Bulletin de sécurité SUSE SUSE-SR:2006:001 du 13 janvier 2006 :  
[http://www.novell.com/linux/security/advisories/2006\\_01\\_sr.html](http://www.novell.com/linux/security/advisories/2006_01_sr.html)
- Bulletin de sécurité Mandriva MDKSA-2006:016 du 16 janvier 2006 :  
<http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:016>
- Bulletin de sécurité Debian DSA-947 du 20 janvier 2006 :  
<http://www.debian.org/security/2006/dsa-947>
- Référence CVE CVE-2006-0162 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0162>

### Gestion détaillée du document

**10 janvier 2006** version initiale.

**16 janvier 2006** ajout des références aux bulletins de sécurité Gentoo, FreeBSD, SUSE et de la référence CVE.

**17 janvier 2006** ajout de la référence au bulletin de sécurité Mandriva.

**20 janvier 2006** ajout de la référence au bulletin de sécurité Debian.

**08 mars 2006** ajout de la référence au bulletin de sécurité OpenBSD.