

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités 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-2005-AVI-348>

---

### Gestion du document

Référence	CERTA-2005-AVI-348-003
Titre	Multiples vulnérabilités dans ClamAV
Date de la première version	19 septembre 2005
Date de la dernière version	29 septembre 2005
Source(s)	Bulletin de mise à jour ClamAV du 16 septembre 2005
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

- Déni de service ;
- exécution potentielle de code arbitraire à distance.

## 2 Systèmes affectés

ClamAV versions 0.86.2 et antérieures.

## 3 Résumé

Deux vulnérabilités dans ClamAV permettent à un utilisateur distant mal intentionné de provoquer un déni de service ou, potentiellement, d'exécuter du code arbitraire.

## 4 Description

Deux vulnérabilités sont présentes dans ClamAV :

- la première est due à une erreur dans la fonction d'analyse des exécutables compressés à l'aide de l'utilitaire UPX (Ultimate Packer for eXecutables).

- la deuxième vulnérabilité est due à une erreur dans la fonction d'analyse des exécutables compressés à l'aide de l'utilitaire FSG .

Ces deux vulnérabilités permettent à un utilisateur distant mal intentionné de provoquer un déni de service ou, potentiellement, d'exécuter du code arbitraire par le biais d'un exécutable malicieusement construit avec UPX ou FSG.

## 5 Solution

Mettre à jour le logiciel en passant à la version 0.87 disponible à l'adresse suivante :  
[http://sourceforge.net/project/showfiles.php?group\\_id=86638&release\\_id=356974](http://sourceforge.net/project/showfiles.php?group_id=86638&release_id=356974)

## 6 Documentation

- Site Internet de ClamAV :  
<http://www.clamav.net>
- Bulletin de mise à jour ClamAV du 16 septembre 2005 :  
[http://sourceforge.net/project/showfiles.php?release\\_id=356974](http://sourceforge.net/project/showfiles.php?release_id=356974)
- Bulletin de sécurité Gentoo GLSA 200509-13 du 19 septembre 2005 :  
<http://www.gentoo.org/security/en/glsa/glsa-200509-13.xml>
- Bulletin de sécurité Mandriva MDKSA-2005:166 du 20 septembre 2005 :  
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:166>
- Bulletin de sécurité FreeBSD pour clamav et clamav-devel du 24 septembre 2005 :  
<http://www.vuxml.org/freebsd/pkg-clamav.html>  
<http://www.vuxml.org/freebsd/pkg-clamav-devel.html>
- Bulletin de sécurité SUSE SUSE-SA:2005:055 du 26 septembre 2005 :  
[http://www.novell.com/linux/security/advisories/2005\\_55\\_clamav.html](http://www.novell.com/linux/security/advisories/2005_55_clamav.html)
- Bulletin de sécurité Debian DSA-824 du 29 septembre 2005 :  
<http://www.debian.org/security/2005/dsa-824>
- Référence CVE CAN-2005-2919 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2919>
- Référence CVE CAN-2005-2920 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2920>

## Gestion détaillée du document

**19 septembre 2005** version initiale.

**22 septembre 2005** ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:166 et aux références CVE CAN-2005-2919 et CAN-2005-2920.

**26 septembre 2005** ajout des références aux bulletins de sécurité FreeBSD et SUSE.

**29 septembre 2005** ajout de la référence aux bulletin de sécurité Debian.