



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 08 avril 2004  
N° CERTA-2004-AVI-098-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

**Objet : Vulnérabilité de 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-2004-AVI-098>

---

### Gestion du document

Référence	CERTA-2004-AVI-098-001
Titre	Vulnérabilité de Clamav
Date de la première version	23 mars 2004
Date de la dernière version	08 avril 2004
Source(s)	Avis de sécurité Secunia SA11177
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.

### 2 Systèmes affectés

Toutes les versions de Clamav antérieures à la version 0.70-rc.

### 3 Résumé

Une vulnérabilité dans Clamav permet à un utilisateur mal intentionné de réaliser un déni de service.

### 4 Description

Clamav est un logiciel libre permettant d'analyser des fichiers à la recherche de virus. Il est souvent utilisé pour détecter les éventuels virus contenus dans les messages arrivant sur un serveur de messagerie. Une vulnérabilité dans le traitement de certains fichiers (archives au format RAR) permet à un utilisateur mal intentionné, par le biais d'une archive habilement constituée, de provoquer un arrêt brutal du service.

## 5 Solution

Mettre à jour Clamav en version 0.70-rc. Site internet de téléchargement de Clamav :  
<http://prdownloads.sourceforge.net/clamav/>

## 6 Documentation

- Site internet de Clamav :  
<http://www.clamav.net>
- Avis de sécurité Secunia SA11177 :  
<http://secunia.com/advisories/11177/>
- Bulletin de sécurité GLSA 200404-07 de Gentoo :  
<http://www.gentoo.org/security/en/glsa/glsa-200404-07.xml>

## Gestion détaillée du document

**23 mars 2004** version initiale.

**08 avril 2004** ajout référence au bulletin de sécurité de Gentoo.