



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 12 mai 2004  
N° CERTA-2004-AVI-161

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-161>

---

### Gestion du document

Référence	CERTA-2004-AVI-161
Titre	Vulnérabilité de Clamav
Date de la première version	12 mai 2004
Date de la dernière version	–
Source(s)	Avis de sécurité Gentoo GLSA 200405-03
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.

### 2 Systèmes affectés

Toutes les versions de Clamav antérieures à la version 0.70.

### 3 Résumé

Une vulnérabilité dans Clamav permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

### 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 liée à la directive `VirusEvent` du fichier de configuration `clamav.conf` permet à un utilisateur mal intentionné, par le biais d'un virus au nom malicieusement constitué, d'exécuter du code arbitraire à distance.

## **5 Solution**

Mettre à jour Clamav en version 0.70 (cf. section Documentation).  
Site internet de téléchargement de Clamav :  
<http://prdownloads.sourceforge.net/clamav/>

## **6 Documentation**

- Site Internet de Clamav :  
<http://www.clamav.net>
- Bulletin de sécurité Gentoo GLSA 200405-03 du 11 mai 2004 :  
<http://www.gentoo.org/security/en/glsa/glsa-200405-03.xml>

## **Gestion détaillée du document**

**12 mai 2004** version initiale.