



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 avril 2009
N° CERTA-2009-AVI-131-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités 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-2009-AVI-131>

Gestion du document

Référence	CERTA-2009-AVI-131-001
Titre	Vulnérabilités de ClamAV
Date de la première version	08 avril 2009
Date de la dernière version	09 avril 2009
Source(s)	Bulletin de sécurité Ubuntu USN-754-1 du 07 avril 2009
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

- Dénis de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

ClamAV, versions inférieures à 0.95.

3 Résumé

Plusieurs vulnérabilités de ClamAV permettent à un utilisateur malveillant de contourner la politique de sécurité ou de provoquer un déni de service.

4 Description

Plusieurs vulnérabilités affectent ClamAV :

- une erreur dans le traitement des archives au format RAR permet à un utilisateur malveillant d'éviter l'analyse de l'archive ;

- une erreur dans le traitement des archives au format TAR permet à un utilisateur malveillant de provoquer une boucle infinie ;
- une erreur dans le traitement des exécutables au format PE permet de provoquer un arrêt inopiné (*crash*), en provoquant une division par zéro.

5 Solution

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

6 Documentation

- Bulletins de sécurité du projet ClamAV :
 - https://www.clamav.net/bugzilla/show_bug.cgi?id=1335
 - https://www.clamav.net/bugzilla/show_bug.cgi?id=1462
 - https://www.clamav.net/bugzilla/show_bug.cgi?id=1467
- Bulletin de sécurité Ubuntu USN-754-1 du 07 avril 2009 :
<http://lists.ubuntu.com/archives/ubuntu-security-announce/2009-April/000880.html>
- Référence CVE CVE-2009-1241 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1241>

Gestion détaillée du document

08 avril 2009 version initiale.

09 avril 2009 corrections d'adresses.