Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 octobre 2011
N° CERTA-2011-AVI-575

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans ClamAV

Gestion du document

Référence	CERTA-2011-AVI-575
Titre	Vulnérabilité dans ClamAV
Date de la première version	19 octobre 2011
Date de la dernière version	–
Source(s)	Correctif ClamAV sous référence bb #3706 du 08 octobre 2011
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 à distance.

2 Systèmes affectés

ClamAV version 0.97.2 et potentiellement les versions antérieures.

3 Résumé

Une vulnérabilité a été corrigée dans ClamAV, qui peut être exploitée pour réaliser un déni de service.

4 Description

Une vulnérabilité a été corrigée dans les fonctions de traitement par niveaux récursifs de ClamAV. En incitant l'analyse par ClamAV d'un fichier spécialement conçu, un attaquant peut causer un arrêt inopiné du logiciel. Il est possible que cette vulnérabilité puisse également être exploitée par l'attaquant pour exécuter du code arbitraire.

5 Solution

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

6 Documentation

– Correctif ClamAV sous référence bb #3706 du 08 octobre 2011 :
http://git.clamav.net/gitweb?p=clamav-devel.git;a=commitdiff;h=3d664817f6ef833a17414a4ecea42004c35cc42f

Gestion détaillée du document

19 octobre 2011 version initiale.