Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 février 2011
N° CERTA-2011-AVI-097

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans ClamAV

Gestion du document

Référence	CERTA-2011-AVI-097
Titre	Vulnérabilité dans ClamAV
Date de la première version	22 février 2011
Date de la dernière version	–
Source(s)	Entrée 2486 du bugzilla de ClamAV du 11/02/2011
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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

ClamAV 0.x

3 Résumé

Une vulnérabilité dans `ClamAV` peut être exploitée par un attaquant distant malveillant pour provoquer un déni de service ou de l'exécution de code arbitraire.

4 Description

Une vulnérabilité, de type libération de pointeur nul, a été corrigée dans la fonction *vba_read_projects_strings* de `ClamAV`. Cette vulnérabilité peut être utilisée, à l'aide d'un fichier spécialement conçu, pour provoquer un déni de service ou de l'exécution de code arbitraire à distance.

5 Solution

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

6 Documentation

– Entrée 2486 du bugzilla de ClamAV du 11/02/2011 :
https://wwws.clamav.net/bugzilla/show_bug.cgi?id=2486

Gestion détaillée du document

22 février 2011 version initiale.