



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 février 2008
N° CERTA-2008-AVI-083

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans 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-2008-AVI-083>

Gestion du document

Référence	CERTA-2008-AVI-083
Titre	Multiples vulnérabilités dans ClamAV
Date de la première version	13 février 2008
Date de la dernière version	–
Source(s)	Mise à jour ClamAV du 11 février 2008
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 versions antérieures à la version 0.92.1.

3 Résumé

Plusieurs vulnérabilités ont été découvertes dans le logiciel antivirus ClamAV. L'exploitation de ces vulnérabilités conduit à l'exécution de commandes arbitraires ou à un déni de service à distance.

4 Description

Deux vulnérabilités ont été découvertes dans le logiciel antivirus ClamAV :

- la première vulnérabilité est due à une erreur dans une fonction de *pe.c*. Cette fonction peut être exploitée par un fichier PE (*Portable Executable*) spécialement construit;

- la seconde vulnérabilité est due à une erreur dans une fonction de *mew.c*.

L'exploitation de l'une ou l'autre de ces vulnérabilités permet de provoquer un déni de service ou d'exécuter des commandes arbitraires à distance.

5 Solution

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

6 Documentation

- Mise à jour de ClamAV du 11 février 2008:
http://sourceforge/project/shownotes.php?release_id=575703
- Bulletin de sécurité iDefense 658 du 13 février 2008 :
<http://www.iddefense.com/ntelligence/vulnerabilities/display.php?id=658>
- Référence CVE CVE-2008-0318 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0318>
- Référence CVE CVE-2008-0728 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0728>

Gestion détaillée du document

13 février 2008 version initiale.