

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-206>

Gestion du document

Référence	CERTA-2008-AVI-206
Titre	Multiples vulnérabilités dans ClamAV
Date de la première version	15 avril 2008
Date de la dernière version	–
Source(s)	Bulletins de sécurité ClamAV du 14 avril 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

- Déni de service à distance.
- Exécution de code arbitraire à distance.

2 Systèmes affectés

ClamAV versions 0.92.x et antérieures.

3 Résumé

De multiples vulnérabilités présentes dans ClamAV permettent à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

Plusieurs erreurs ont été identifiées dans l'antivirus ClamAV :

- la première concerne l'analyseur de fichiers exécutables au format PE engendrés par le « *packer* » : Upack ;

- la seconde concerne l'analyseur de fichiers exécutables au format PE engendrés par un autre « *packer* » : *SpinPE* ;
- la dernière est relative à l'analyseur de fichiers compressés au format ARJ.

Les deux premières vulnérabilités permettent à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire. Quant à la dernière, elle permet de provoquer un déni de service de l'antivirus vulnérable.

5 Solution

La version 0.93 de ClamAV corrige le problème :

<http://www.clamav.net/download/sources>

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

6 Documentation

- Site de ClamAV :
<http://www.clamav.net>
- Bulletin de sécurité ClamAV :
http://www.clamav.net/bugzilla/show_bug.cgi?id=878
http://www.clamav.net/bugzilla/show_bug.cgi?id=876
http://www.clamav.net/bugzilla/show_bug.cgi?id=897
- Référence CVE CVE-2008-1100 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1100>
- Référence CVE CVE-2008-1387 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1387>

Gestion détaillée du document

15 avril 2008 version initiale.