Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 juillet 2008
N° CERTA-2008-AVI-382

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de l'antivirus ClamAV

Gestion du document

Référence	CERTA-2008-AVI-382
Titre	Multiples vulnérabilités de l'antivirus ClamAV
Date de la première version	29 juillet 2008
Date de la dernière version	–
Source(s)	Note de version ClamAV du 07 juillet 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.

2 Systèmes affectés

ClamAV versions antérieures à la version 0.93.3.

3 Résumé

Deux vulnérabilités ont été découvertes dans l'antivirus `ClamAV`. L'exploitation de ces vulnérabilités permet de réaliser un déni de service à distance.

4 Description

Deux vulnérabilités résultant d'une mauvaise gestion aux limites ont été découvertes dans le traitement par `ClamAV` des fichiers modifiés par le *packer* `Petite`. L'exploitation de cette vulnérabilité permet de réaliser un déni de service sur l'antivirus.

5 Solution

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

6 Documentation

- Publication de mises à jour ClamAV numéros 605577 et 611890 :
  http://sourceforge.net/project/shownotes.php?release_id=605577&group_id=86638
  http://sourceforge.net/project/shownotes.php?release_id=611890&group_id=86638
- Bulletin de sécurité Debian DSA 1616 du 26 juillet 2008 :
  http://www.debian.org/security/2008/dsa-1616
- Mises à jour de sécurité Fedora FEDORA-2008-5476 et FEDORA-2008-6422 :
  https://www.redhat.com/archives/fedora-package-announce/2008-June/msg00763.html
  https://www.redhat.com/archives/fedora-package-announce/2008-June/msg00617.html
- Bulletin de sécurité Mandriva MDVSA-2008:122 du 24 juin 2008 :
  http://www.mandriva.com/security/advisories?name=MDVSA-2008:122
- Référence CVE CVE-2008-2713 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2713
- Référence CVE CVE-2008-3215 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3215

Gestion détaillée du document

29 juillet 2008 version initiale.