

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-2011-AVI-415>

Gestion du document

Référence	CERTA-2011-AVI-415
Titre	Vulnérabilité dans ClamAV
Date de la première version	27 juillet 2011
Date de la dernière version	–
Source(s)	Notes de version ClamAV 0.97.2 du 25 juillet 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 jusqu'à la version 0.97.2.

3 Résumé

Une vulnérabilité découverte dans ClamAV permet à une personne malveillante de provoquer un déni de service à distance.

4 Description

Une vulnérabilité a été corrigée dans ClamAV. Cette vulnérabilité peut être exploitée par une personne malveillante, à l'aide d'un courriel spécialement conçu, pour provoquer un déni de service du démon *clamd*.

5 Solution

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

6 Documentation

- Notes de version ClamAV 0.97.2 du 25 juillet 2011 :
<http://blog.clamav.net/2011/07/clamav-0972-is-now-available.html>

Gestion détaillée du document

27 juillet 2011 version initiale.