



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 décembre 2008
N° CERTA-2008-AVI-574-002

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-2008-AVI-574>

Gestion du document

Référence	CERTA-2008-AVI-574-002
Titre	Vulnérabilité dans ClamAV
Date de la première version	02 décembre 2008
Date de la dernière version	16 décembre 2008
Source(s)	Note de version 0.94.2 de ClamAV
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

Toutes les versions antérieures à la version 0.94.2.

3 Résumé

Une vulnérabilité dans ClamAV permet à une personne malintentionnée d'effectuer un déni de service à distance.

4 Description

Une vulnérabilité dans la fonction `cli_check_jpeg_exploit()` de `special.c` permet à une personne malintentionnée d'effectuer un déni de service à distance.

5 Solution

Utiliser la version 0.94.2.

Télécharger la nouvelle version sur le site de l'éditeur (cf. section Documentation).

6 Documentation

- Site du projet ClamAV :
<http://www.sourceforge.net/projects/clamav/>
- Note de version 0.94.2 de ClamAV :
http://www.sourceforge.net/project/shownotes.php?group_id=86638&release_id=643134
- Bulletin de sécurité Ubuntu USN-684-1 du 02 décembre 2008 :
<http://www.ubuntu.com/usn/usn-684-1>
- Bulletin de sécurité Mandriva MDVSA-2008:239 du 05 décembre 2008 :
<http://www.mandriva.com/security/advisories?name=MDVSA-2008:239>
- Référence CVE CVE-2008-5314 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5314>

Gestion détaillée du document

02 décembre 2008 version initiale ;

03 décembre 2008 ajout de la référence Ubuntu.

16 décembre 2008 ajout de la référence Mandriva et du CVE.