

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-553>

Gestion du document

Référence	CERTA-2008-AVI-553
Titre	Vulnérabilité dans ClamAV
Date de la première version	13 novembre 2008
Date de la dernière version	–
Source(s)	Notes de modifications de la version 0.94.1
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 0.94.1.

3 Résumé

Une vulnérabilité dans ClamAV permet à une personne malintentionnée distante d'effectuer un déni de service voire d'exécuter du code arbitraire.

4 Description

Une vulnérabilité a été identifiée dans la fonction `get_unicode_name()` dans le fichier `vba_extract.c` de ClamAV. Son exploitation peut permettre à une personne malintentionnée distante d'effectuer un déni de service voire d'exécuter du code arbitraire.

5 Solution

La version 0.94.1 de ClamAV corrige ce problème.

6 Documentation

- Site web de ClamAV :
<http://www.clamav.net>
- Notes de modifications de la version 0.94.1 :
http://sourceforge.net/project/shownotes.php?release_id=637952&group_id=86638

Gestion détaillée du document

13 novembre 2008 version initiale.