

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de 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-2007-AVI-306>

Gestion du document

Référence	CERTA-2007-AVI-306-001
Titre	Vulnérabilité de ClamAV
Date de la première version	12 juillet 2007
Date de la dernière version	27 juillet 2007
Source(s)	Rapport de correction d'erreur de ClamAV du 10 juillet 2007
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.

2 Systèmes affectés

ClamAV versions 0.90 et antérieures.

3 Résumé

Une vulnérabilité dans ClamAV permet à un utilisateur distant de provoquer un déni de service de l'application vulnérable.

4 Description

Une erreur de type pointeur nul dans le composant de ClamAV mettant en œuvre l'analyse des fichiers au format RAR permet à un utilisateur distant malintentionné de provoquer un déni de service de l'antivirus vulnérable par le biais d'un fichier RAR construit de façon particulière.

5 Solution

La version 0.91 de ClamAV corrige le problème :
http://sourceforge.net/project/showfiles.php?group_id=86638

6 Documentation

- Site officiel de ClamAV :
<http://www.clamav.net>
- Rapport de correction d'erreur de ClamAV du 10 juillet 2007 :
https://www.clamav.net/bugzilla/show_bug.cgi?id=555
- Bulletin de sécurité Mandriva MDKSA-2007:150 du 25 juillet 2007 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:150>
- Bulletin de sécurité Debian DSA-1340 du 24 juillet 2007 :
<http://www.debian.org/security/2007/dsa-1340>
- Référence CVE CVE-2007-3725 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3725>

Gestion détaillée du document

12 juillet 2007 version initiale.

27 juillet 2007 ajout de la référence CVE et des références aux bulletins de sécurité Mandriva et Debian.