



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 mars 2007
N° CERTA-2007-AVI-093-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités 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-2007-AVI-093>

Gestion du document

Référence	CERTA-2007-AVI-093-002
Titre	Multiples vulnérabilités dans ClamAV
Date de la première version	16 février 2007
Date de la dernière version	13 mars 2007
Source(s)	Bulletins de sécurité iDefense 475 et 476 du 15 février 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

- Contournement de la politique de sécurité ;
- déni de service à distance.

2 Systèmes affectés

- ClamAV version 0.90RC1.1 et antérieures.

3 Résumé

Plusieurs vulnérabilités présentes dans ClamAV permettent à un utilisateur distant de contourner la politique de sécurité ou de réaliser un déni de service.

4 Description

Deux vulnérabilités ont été identifiées dans ClamAV :

- un problème de libération de ressources lors de la validation de l'entête des fichiers de type cabinet (fichier CAB) peut permettre à une personne distante malintentionnée de réaliser un déni de service en bloquant toutes les ressources disponibles ;

- un manque de validation d'un paramètre des entêtes MIME pourrait permettre à un utilisateur malveillant de contourner la politique de sécurité en modifiant des fichiers protégés de l'antivirus.

5 Solution

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

6 Documentation

- Bulletin de sécurité iDefense 475 du 15 février 2007 :
<http://www.iddefense.com/application/poi/display?id=475>
- Bulletin de sécurité iDefense 476 du 15 février 2007 :
<http://www.iddefense.com/application/poi/display?id=476>
- Bulletin Mandriva MDKSA-2007:043 du 19 février 2007 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:043>
- Mise à jour de sécurité Gentoo :
<http://www.gentoo.org/security/en/glsa/glsa-200703-03.xml>
- Mise à jour de sécurité Debian :
<http://lists.debian.org/debian-security-announce/debian-security-announce-2007/msg00018.html>
- Mise à jour de sécurité SuSE :
<http://lists.suse.com/archive/suse-security-announce/2007-Feb/0004.html>
- Référence CVE CVE-2007-0897 :
<http://cve.mitre.org/cgi-bin/cvname.cgi?name=CVE-2007-0897>
- Référence CVE CVE-2007-0898 :
<http://cve.mitre.org/cgi-bin/cvname.cgi?name=CVE-2007-0898>

Gestion détaillée du document

16 février 2007 version initiale ;

21 février 2007 ajout de la référence Mandriva ;

13 mars 2007 ajout des références Debian, SuSE et Gentoo.