Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 décembre 2006
N° CERTA-2006-AVI-553-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de ClamAV

Gestion du document

Référence	CERTA-2006-AVI-553-001
Titre	Vulnérabilité de ClamAV
Date de la première version	14 décembre 2006
Date de la dernière version	19 décembre 2006
Source(s)	CVE-2006-6481
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 0.88.6 et versions antérieures.

3 Résumé

ClamAV est un antivirus en ligne de commande pour les systèmes Unix.
Une vulnérabilité dans l'analyse des courriels à parties MIME imbriquées permet à un utilisateur malintentionné de provoquer un déni de service à distance.

4 Description

Le format MIME (RFC 2045 à 2049, RFC 2077) est une extension du format de courriel qui permet l'intégration des caractères autres que ceux de l'ASCII : caractères accentués, pièces jointes en binaire, messages chiffrés

ou signés. Un message MIME peut contenir plusieurs parties (type MIME `multipart`), par exemple une pour le corps du courriel et une par pièce jointe. Chaque partie peut à son tour contenir plusieurs parties (imbrication).

Lorsque *ClamAV* analyse un courriel de type MIME `multipart` avec de nombreux niveaux d'imbrications, un débordement de mémoire provoque l'arrêt du programme. L'envoi d'un courriel spécialement construit permet à un utilisateur distant de provoquer un déni de service.

5 Solution

Passer à la version 0.88.7 (cf. section Documentation).

6 Documentation

- Site du projet clamav :
  http://www.clamav.net/stable.php
- Bulletin de sécurité Gentoo GLSA-200612-18 du 18 décembre 2006 :
  http://www.gentoo.org/security/en/glsa/glsa-200612-18.xml
- Bulletin de sécurité SuSE SUSE-SA:2006:078 du 18 décembre 2006 :
  http://lists.suse.com/archive/suse-security-announce/2006-Dec/0007.html
- Bulletin de sécurité Debian DSA-1238 du 17 décembre 2006 :
  http://www.us.debian.org/security/2006/dsa-1238
- Bulletin de sécurité Mandriva MDKSA-2006:230 du 13 décembre 2006 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2006:230
- Référence CVE CVE-2006-6481 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6481

Gestion détaillée du document

14 décembre 2006 version initiale.
19 décembre 2006 ajout des références aux bulletins de sécurité Gentoo, SuSE, Debian et Mandriva.