Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 novembre 2006
N° CERTA-2006-AVI-454-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Clam Antivirus

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-2006-AVI-454`

Gestion du document

Référence	CERTA-2006-AVI-454-002
Titre	Vulnérabilités dans Clam Antivirus
Date de la première version	16 octobre 2006
Date de la dernière version	07 novembre 2006
Source(s)	Journal du changement de Clam Antivirus du 15 octobre 2006
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

`Clam antivirus` versions antérieures à `0.88.5`.

3 Résumé

De multiples vulnérabilités dans l'antivirus `Clam Antivirus` peuvent permettre à un utilisateur mal intentionné de réaliser un déni de service.

4 Description

Deux vulnérabilités sont présentes dans `Clam Antivirus`:

– Une vulnérabilité dans la fonction `unpack` pour les fichiers d'aide Microsoft (fichiers `CHM`) peut conduire un utilisateur mal intentionné à réaliser un deni de service.

– Une vulnérabilité dans la reconstruction de fichiers exécutables au format `PE` permet à un utilisateur mal intentionné de réaliser un dépassement de mémoire.

5 Solution

La version 0.88.5 de `Clam Antivirus` corrige le problème.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

– Journal du changement de Clam Antivirus du 15 octobre 2006 :
http://sourceforge.net/project/shownotes.php?release_id=455799
– Bulletin de sécurité Secunia du 16 octobre 2006 :
http://secunia.com/advisories/22370
– Bulletin de sécurité FreeBSD du 16 octobre 20006 :
http://www.vuxml.org/freebsd/pkg-clamav.html
– Bulletin de sécurité Gentoo du 24 octobre 2006 :
http://www.gentoo.org/security/en/glsa/glsa-200610-10.xml
– Bulletin de sécurité Debian du 19 octobre 2006 :
http://www.debian.org/security/2006/dsa-1196
– Bulletin de sécurité Suse du 18 octobre 2006 :
http://www.novell.com/linux/security/advisories/2006_60_clamav.html
– Bulletin de sécurité Mandriva 18 octobre 2006 :
http://www.mandriva.com/security/advisories?name=MDKA-2006:184

Gestion détaillée du document

16 octobre 2006 version initiale ;
17 ocotbre 2006 ajout du bulletin de sécurité FreeBSD ;
07 novembre 2006 ajout des bulletins de sécurité Gentoo, Debian, Suse et Mandriva.