Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 mai 2006
N° CERTA-2006-AVI-176-001

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-2006-AVI-176

Gestion du document

Référence	CERTA-2006-AVI-176-001
Titre	Vulnérabilité dans ClamAV
Date de la première version	03 mai 2006
Date de la dernière version	04 mai 2006
Source(s)	Bulletin de sécurité ClamAV 0.88.2
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 ;
- déni de service.

2 Systèmes affectés

ClamAV versions 0.80 à 0.88.1.

3 Résumé

Une vulnérabilité a été découverte dans *Freshclam* permettant de réaliser un déni de service ou d'exécuter du code arbitraire.

4 Description

Freshclam est un utilitaire de *ClamAV* en ligne de commande permettant de télécharger et d'installer les mises à jour des bases de signatures des virus. Une vulnérabilité a été découverte dans le client HTTP de *Freshclam* lors de la vérification de la taille des en-têtes des données provenant d'un serveur HTTP. L'exploitation de cette

vulnérabilité, qui requiert un serveur HTTP malveillant d'hébergement des bases de signatures, permet de réaliser un déni de service ou d'exécuter du code arbitraire.

5 Solution

Mettre à jour en version 0.88.2 (voir Documentation).

6 Documentation

- Bulletin de sécurité ClamAV 0.88.2 :
  http://www.clamav.net/security/0.88.2.html
- Version 0.88.2 de ClamAV :
  http://www.clamav.net/stable.php#pagestart
- Bulletin de sécurité Gentoo GLSA-200605-03 du 02 mai 2006 :
  http://www.gentoo.org/security/en/glsa/glsa-200605-03.xml
- Bulletin de sécurité Mandriva MDKSA-2006:080 du 01 mai 2006 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2006:080
- Bulletin de sécurité Debian DSA-1050 du 02 mai 2006 :
  http://www.debian.org/security/2006/dsa-1050
- Référence CVE CVE-2006-1989 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1989

Gestion détaillée du document

03 mai 2006 version initiale.

04 mai 2006 ajout des références aux bulletins de sécurité Mandriva, Debian.