

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-2006-AVI-140>

Gestion du document

Référence	CERTA-2006-AVI-140-001
Titre	Multiples vulnérabilités dans ClamAV
Date de la première version	07 avril 2006
Date de la dernière version	10 avril 2006
Source(s)	Mise à jour de sécurité pour ClamAV du 04 avril 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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

Clam AntiVirus 0.88 et versions antérieures.

3 Résumé

Plusieurs vulnérabilités dans ClamAV permettent à un utilisateur distant mal intentionné de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

ClamAV est un logiciel antivirus libre (GPL).

Trois types de vulnérabilités ont été découvertes dans ClamAV :

- une vulnérabilité de type débordement d'entier dans le traitement des en-tête PE ;

- plusieurs vulnérabilités de type chaîne de format peuvent être exploitées à distance afin d'exécuter du code arbitraire ;
- une vulnérabilité de type débordement de mémoire dans la fonction `cli_bitset_set()` peut être exploitée afin de provoquer un déni de service.

5 Solution

Appliquer la mise à jour de sécurité de ClamAV en passant à la version 0.88.1 disponible à l'adresse suivante : http://sourceforge.net/project/showfiles.php?group_id=86638&release_id=407078
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Mise à jour de sécurité pour ClamAV en version 0.88.1 :
http://sourceforge.net/project/showfiles.php?group_id=86638&release_id=407078
- Bulletin de sécurité Debian DSA 1024 du 05 avril 2006 :
<http://www.debian.org/security/2006/dsa-1024>
- Bulletin de sécurité Mandriva MDKSA-2006:067 du 07 avril 2006 :
<http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2006:067>
- Bulletin de sécurité Gentoo GLSA-200604-06.xml du 07 avril 2006 :
<http://www.gentoo.org/security/en/glsa/glsa-200604-06.xml>
- Bulletin de sécurité FreeBSD du 06 avril 2006 :
<http://www.vuxml.org/freebsd/pkg-clamav.html>
- Référence CVE CAN-2006-1614 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-1614>
- Référence CVE CAN-2006-1615 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-1615>
- Référence CVE CAN-2006-1630 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-1630>

Gestion détaillée du document

07 avril 2006 version initiale.

10 avril 2006 ajout des références aux bulletins de sécurité Mandriva, Gentoo et FreeBSD.