

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-2005-AVI-437>

Gestion du document

Référence	CERTA-2005-AVI-437-001
Titre	Multiples vulnérabilités dans ClamAV
Date de la première version	07 novembre 2005
Date de la dernière version	08 novembre 2005
Source(s)	Bulletin de sécurité ClamAV
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 ;
- exécution potentielle de code arbitraire à distance.

2 Systèmes affectés

ClamAV versions 0.87 et antérieures.

3 Résumé

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

4 Description

Trois vulnérabilités sont présentes dans ClamAV :

- la première est due à une erreur dans la fonction d'analyse des exécutables compressés à l'aide de l'utilitaire FSG ;

- la deuxième est due à une erreur dans la fonction d'analyse des fichiers au format TNEF ;
- la troisième est due à une erreur dans la fonction d'analyse des archives au format CAB.

Ces trois vulnérabilités permettent à un utilisateur distant mal intentionné de provoquer un déni de service ou, potentiellement, d'exécuter du code arbitraire par le biais de fichiers malicieusement construits.

5 Solution

Mettre à jour le logiciel en passant à la version 0.87.1 disponible à l'adresse suivante :

http://sourceforge.net/project/showfiles.php?group_id=86638&release_id=368319

6 Documentation

- Site Internet de ClamAV :
<http://www.clamav.net>
- Mise à jour ClamAV du 03 novembre 2005 :
http://sourceforge.net/project/showfiles.php?release_id=368319
- Bulletin de sécurité Gentoo GLSA 200511-04 du 06 novembre 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200511-04.xml>
- Bulletin de sécurité Debian DSA-887 du 07 novembre 2005 :
<http://www.debian.org/security/2005/dsa-887>
- Bulletin de sécurité Mandriva MDKSA-2005:205 du 07 novembre 2005 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:205>
- Référence CVE CAN-2005-3239 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3239>
- Référence CVE CAN-2005-3303 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3303>
- Référence CVE CAN-2005-3500 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3500>
- Référence CVE CAN-2005-3501 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3501>

Gestion détaillée du document

07 novembre 2005 version initiale.

08 novembre 2005 ajout des références CVE et des bulletins de sécurité Debian et Mandriva.