Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 juillet 2005
N° CERTA-2005-AVI-234-004

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de ClamAV

Gestion du document

Référence	CERTA-2005-AVI-234-004
Titre	Vulnérabilité de ClamAV
Date de la première version	28 juin 2005
Date de la dernière version	12 juillet 2005
Source(s)	Bulletin de sécurité Gentoo GLSA 200506-23
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

Toutes les versions de ClamAV antérieures à la version 0.86.1.

3 Résumé

Une vulnérabilité dans ClamAV permet à un utilisateur mal intentionné de réaliser un déni de service sur la plate-forme vulnérable.

4 Description

ClamAV est un logiciel libre permettant d'analyser des fichiers à la recherche de signatures de virus. Il est souvent utilisé pour détecter les éventuels virus contenus dans les messages arrivant sur un serveur de messagerie.

- Une vulnérabilité dans la fonction `cli_msexpand` permettant la décompression de certains fichiers permet à un utilisateur mal intentionné, par le biais d'un fichier habilement constitué, de provoquer un arrêt brutal du service (CVE CAN-2005-1922) ;
- Une vulnérabilité dans le traitement de certains fichiers (archives au format CAB) permet à un utilisateur mal intentionné, par le biais d'une archive habilement constituée, de provoquer un arrêt brutal du service (CVE CAN-2005-1923) ;
- Une vulnérabilité dans le traitement de certains fichiers (archives au format Quantum) permet à un utilisateur mal intentionné, par le biais d'une archive habilement constituée, de provoquer un arrêt brutal du service (CVE CAN-2005-2056) ;
- Une vulnérabilité dans la partie filtre de messages électroniques de ClamAV (`clamav-milter`) permet à un utilisateur mal intentionné de provoquer un arrêt brutal du service (CVE CAN-2005-2070).

5 Solution

Mettre à jour ClamAV en version 0.86.1. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site Internet de ClamAV :
  http://www.clamav.net
- Annonce de la sortie de la version 0.86 de ClamAV :
  http://sourceforge.net/project/shownotes.php?release_id=336462
- Annonce de la sortie de la version 0.86.1 de ClamAV :
  http://sourceforge.net/project/shownotes.php?release_id=337279
- Bulletin de sécurité iDEFENSE id=275 06.29.05 :
  http://www.idefense.com/application/poi/display?id=275&type=vulnerabilities
- Bulletin de sécurité iDEFENSE id=276 06.29.05 :
  http://www.idefense.com/application/poi/display?id=276&type=vulnerabilities
- Bulletin de sécurité OpenBSD du 28 juin 2005 :
  http://www.vuxml.org/openbsd/pkg-clamav.html
- Bulletin de sécurité Gentoo GLSA 200506-23 du 27 juin 2005 :
  http://www.gentoo.org/security/en/glsa/glsa-200506-23.xml
- Bulletin de sécurité SUSE SUSE-SA:2005:038 du 29 juin 2005 :
  http://www.novell.com/linux/security/advisories/2005_38_clamav.html
- Bulletin de sécurité Debian DSA-737 du 05 juillet 2005 :
  http://www.debian.org/security/2005/dsa-737
- Bulletins de sécurité FreeBSD pour clamav et clamav-devel du 06 juillet 2005 :
  http://www.vuxml.org/freebsd/pkg-clamav.html
- Bulletin de sécurité Mandriva MDKSA-2005:113 du 11 juillet 2005 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2005:113
- Référence CVE CAN-2005-1922 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1922
- Référence CVE CAN-2005-1923 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1923
- Référence CVE CAN-2005-2056 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2056
- Référence CVE CAN-2005-2070 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2070

Gestion détaillée du document

28 juin 2005 version initiale.

30 juin 2005 ajout de la référence au bulletin de sécurité OpenBSD.

06 juillet 2005 ajout de trois vulnérabilités, des quatre références CVE (CAN-2005-1922, CAN-2005-1923, CAN-2005-2056 et CAN-2005-2070), de la référence au bulletin de sécurité Debian DSA-737, de la référence au bulletin de sécurité SUSE-SA:2005:038, de la référence à l'annonce de la sortie de ClamAV 0.86, des deux bulletins de sécurité iDEFENSE.

07 juillet 2005 ajout des références aux bulletins de sécurité FreeBSD.

12 juillet 2005 ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:113.