Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 février 2005
N° CERTA-2005-AVI-044-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de ClamAV

Gestion du document

Référence	CERTA-2005-AVI-044-001
Titre	Vulnérabilité de ClamAV
Date de la première version	01 février 2005
Date de la dernière version	24 février 2005
Source(s)	Bulletin de sécurité Gentoo GLSA 200501-46
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

- Contournement de la politique de sécurité ;
- déni de service.

2 Systèmes affectés

`ClamAV` versions 0.80 et antérieures.

3 Résumé

Deux vulnérabilités dans `ClamAV` permettent à un utilisateur mal intentionné de contourner la politique de sécurité ou 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 virus. Il est souvent utilisé pour détecter les éventuels virus contenus dans les messages arrivant sur un serveur de messagerie.
Une vulnérabilité dans le traitement des entêtes de certains fichiers (archives au format ZIP) permet à un utilisateur

mal intentionné, par le biais d'une archive habilement constituée, de provoquer un arrêt brutal du service.
Une seconde vulnérabilité dans le traitement des URL contenant une image encodée au format `base64` permet à un utilisateur mal intentionné de contourner la politique de sécurité en créant un fichier qui va échapper à l'analyse de `ClamAV`.

5 Solution

Mettre à jour `ClamAV` en version 0.81.
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 0.81 de `ClamAV` :
  http://sourceforge.net/forum/forum.php?forum_id=440649
- Bulletin de sécurité Gentoo GLSA 200501-46 du 31 janvier 2005 :
  http://www.gentoo.org/security/en/glsa/glsa-200501-46.xml
- Bulletin de sécurité Mandrake MDKSA-2005:025 du 31 janvier 2005 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:025
- Mise à jour de sécurité du paquetage NetBSD clamav :
  ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/mail/clamav/README.html
- Référence CVE CAN-2005-0133 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0133

Gestion détaillée du document

01 février 2005 version initiale.
24 février 2005 ajout de la référence au bulletin de sécurité NetBSD.