Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 31 décembre 2007
N° CERTA-2007-AVI-552-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans ClamAV

Gestion du document

Référence	CERTA-2007-AVI-552-001
Titre	Vulnérabilité dans ClamAV
Date de la première version	19 décembre 2007
Date de la dernière version	31 décembre 2007
Source(s)	Bulletin de sécurité iDefense 634 du 18 décembre 2007
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.

2 Systèmes affectés

ClamAV versions 0.91.2 et antérieures.

3 Résumé

Des vulnérabilités dans *ClamAV* permettent l'exécution de code arbitraire à distance.

4 Description

Des vulnérabilités ont été découvertes dans les modules *ClamAV* de traitement des archives au format *MEW* et *bzip2*. Un utilisateur malintentionné peut, par le biais d'un fichier compressé, exécuter du code arbitraire à distance.

5 Solution

Mettre à jour *ClamAV* en version 0.92 (cf. section Documentation).

6 Documentation

- Version 0.92 de *ClamAV* :
  http://www.clamav.net/download/sources/
- Bulletin de sécurité iDefense 634 du 18 décembre 2007 :
  http://www.idefense.com/ntelligence/vulnerabilities/display.php?id=634
- Bulletin de sécurité *Gentoo* 200712-20 du 29 décembre 2007 :
  http://www.gentoo.org/security/en/glsa-200712-20.xml
- Bulletin de sécurité *Debian* DSA-1535-1 du 19 décembre 2007 :
  http://www.debian.org/security/2007/dsa-1435
- Référence CVE CVE-2007-5759 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5759
- Référence CVE CVE-2007-6335 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6335
- Référence CVE CVE-2007-6336 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6336
- Référence CVE CVE-2007-6337 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6337

Gestion détaillée du document

19 décembre 2007 version initiale ;
31 décembre 2007 Ajout des références CVE et des bulletins de sécurité de *Gentoo* et *Debian*.