

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : 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-2010-AVI-576>

Gestion du document

Référence	CERTA-2010-AVI-576-001
Titre	Vulnérabilités dans ClamAV
Date de la première version	03 décembre 2010
Date de la dernière version	10 décembre 2010
Source(s)	Site des sources de 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 à distance.

2 Systèmes affectés

ClamAV 0.96.4 et versions antérieures.

3 Résumé

Deux vulnérabilités dans ClamAV permettent à un utilisateur malveillant de provoquer un déni de service à distance.

4 Description

Deux vulnérabilités ont été corrigées dans ClamAV :

- une erreur dans le traitement des fichiers au format PDF permet de provoquer un arrêt inopiné ;
- une erreur dans la fonction `icon_cb()` permet de corrompre la mémoire.

5 Solution

La version 0.96.5 remédie à ces problèmes.

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site des sources de ClamAV :
<http://git.clamav.net/>
- Bulletin de sécurité Fedora FEDORA-2010-18568 du 07 décembre 2010 :
<http://lists.fedoraproject.org/pipermail/package-announce/2010-December/051905.html>
- Bulletin de sécurité Mandriva MDVSA-2010:249 du 07 décembre 2010 :
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:249>
- Bulletin de sécurité Ubuntu USN-1031-1 du 10 décembre 2010 :
<http://www.ubuntu.com/usn/usn-1031-1>
- Référence CVE CVE-2010-4260 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4260>
- Référence CVE CVE-2010-4261 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4261>
- Référence CVE CVE-2010-4479 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4479>

Gestion détaillée du document

03 décembre 2010 version initiale.

10 décembre 2010 ajout des références aux bulletins Fedora, Mandriva et Ubuntu, et des CVE.