Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 décembre 2008
N° CERTA-2008-AVI-575

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans imlib2

Gestion du document

Référence	CERTA-2008-AVI-575
Titre	Vulnérabilité dans imlib2
Date de la première version	03 décembre 2008
Date de la dernière version	–
Source(s)	
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 ;
- déni de service à distance.

2 Systèmes affectés

imlib2 1.4.2 et versions antérieures.

3 Résumé

Une vulnérabilité dans la bibliothèque `imlib2` permet à une personne malintentionnée distante de provoquer un déni de service ou potentiellement d'exécuter du code arbitraire.

4 Description

Une vulnérabilité de type débordement de mémoire a été corrigée dans la fonction *load()* utilisée pour le chargement de fichiers `XPM` dans `imlib2`. L'exploitation de cette vulnérabilité via un fichier spécialement conçu permet à une personne malintentionnée distante de provoquer un déni de service ou potentiellement d'exécuter du code arbitraire sur une application utilisant cette bibliothèque.

5 Solution

Se référer aux bulletins de sécurité des éditeurs pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Debian DSA 1672 du 29 novembre 2008 :
  http://www.debian.org/security/2008/dsa-1672
- Bulletin de sécurité Ubuntu 683-1 du 02 décembre 2008 :
  http://www.ubuntu.com/usn/USN-683-1
- Bulletin de sécurité Fedora 8 FEDORA-2008-10296 du 26 novembre 2008 :
  http://www.redhat.com/archives/fedora-package-announce/2008-November/msg00858.html
- Bulletin de sécurité Fedora 9 FEDORA-2008-10287 du 26 novembre 2008 :
  http://www.redhat.com/archives/fedora-package-announce/2008-November/msg00856.html
- Bulletin de sécurité Fedora 10 FEDORA-2008-10364 du 26 novembre 2008 :
  http://www.redhat.com/archives/fedora-package-announce/2008-November/msg00906.html
- Référence CVE CVE-2008-5187 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5187

Gestion détaillée du document

03 décembre 2008 version initiale.