Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 novembre 2007
N° CERTA-2007-AVI-479

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de GNU Emacs

Gestion du document

Référence	CERTA-2007-AVI-479
Titre	Vulnérabilité de GNU Emacs
Date de la première version	06 novembre 2007
Date de la dernière version	–
Source(s)	Rapport d'erreur Debian 449008
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

GNU Emacs, versions 22.x.

3 Résumé

Une erreur dans le traitement de certains fichiers permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Une erreur de traitement dans la fonction `hack-local-variables` est exploitable par un utilisateur malveillant pour modifier le fichier `user-init-file` d'un utilisateur et ensuite exécuter du code Lisp pour Emacs.

La vulnérabilité n'est exploitable que si le paramètre `enable-local-variables` est positionné à `:safe`.

5 Solution

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

6 Documentation

- Rapport d'erreur Debian 449008 :
  http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=449008
- Site du CVS Emacs :
  http://cvs.savannah.gnu.org/viewvc/emacs/emacs/lisp/files.el?r1=1.896.2.28&r2=1.896.2.29
- Référence CVE CVE-2007-5795 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5795

Gestion détaillée du document

06 novembre 2007 version initiale.