



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 février 2008
N° CERTA-2008-AVI-084

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de PCRE

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-2008-AVI-084>

Gestion du document

| | |
|-----------------------------|-----------------------|
| Référence | CERTA-2008-AVI-084 |
| Titre | Vulnérabilité de PCRE |
| Date de la première version | 14 février 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

- Déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

PCRE, version 7.5 et versions précédentes.

3 Résumé

Une vulnérabilité de PCRE permettrait à un utilisateur malveillant de provoquer un déni de service à distance ou de compromettre une application utilisant PCRE.

4 Description

PCRE est une bibliothèque utilisant la même syntaxe et la même sémantique que Perl pour traiter les expressions régulières.

Un défaut de vérification de borne dans PCRE permet de réaliser un débordement de mémoire (*buffer overflow*). Cette vulnérabilité permettrait à un utilisateur malveillant de provoquer un déni de service à distance ou de compromettre une application utilisant PCRE.

5 Solution

La version 7.6 résoud ce problème. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Notes de version PCRE du 28 janvier 2008 :
<http://pcre.org/changelog.txt>
- Bulletin de bogue Redhat 431660 du 06 février 2008 :
https://bugzilla.redhat.com/show_.cgi?id=431660
- Référence CVE CVE-2008-0674 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0674>

Gestion détaillée du document

14 février 2008 version initiale.