

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 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-361>

Gestion du document

Référence	CERTA-2008-AVI-361
Titre	Vulnérabilité dans PCRE
Date de la première version	10 juillet 2008
Date de la dernière version	–
Source(s)	CVE-2008-2371
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

Bibliothèque *PCRE*, version 7.7 et versions antérieures.
Des applications et des bibliothèques reposant sur *PCRE*, comme *GNOME glib*, peuvent être concernées.

3 Résumé

Une vulnérabilité de type débordement de mémoire permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

PCRE est une bibliothèque de traitement d'expressions régulières.

Une erreur est présente dans le traitement des motifs comprenant plusieurs branches et commençant par un optionnel au début. Elle peut provoquer un débordement de mémoire. L'exploitation de cette vulnérabilité permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

5 Solution

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

6 Documentation

- Bulletin de sécurité Debian DSA 1602 du 05 juillet 2008 :
<http://www.debian.org/security/2008/dsa-1602>
- Bulletins de sécurité Fedora du 06 juillet 2008 :
<https://www.redhat.com/archives/fedora-package-announce/2008-July/msg00181.html>
<https://www.redhat.com/archives/fedora-package-announce/2008-July/msg00182.html>
- Bulletin de sécurité Gentoo GLSA-200807-03 du 07 juillet 2008 :
<http://www.gentoo.org/security/en/glsa/glsa-200807-03.xml>
- Bulletin de sécurité OpenSuse du 04 juillet 2008 :
<http://lists.opensuse.org/opensuse-security-announce/2008-07/msg00001.html>
- Bulletin de version GNOME du 30 juin 2008 :
<http://ftp.gnome.org/pub/GNOME/sources/glib/2.16/glib-2.16.4.changes/>
- Référence CVE CVE-2008-2371 :
<http://cve.mitre.org/cgi-bin/cvname.cgi?name=CVE-2008-2371>

Gestion détaillée du document

10 juillet 2008 version initiale.