

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de la bibliothèque 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-2007-AVI-513>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2007-AVI-513 |
| Titre | Multiples vulnérabilités de la bibliothèque PCRE |
| Date de la première version | 30 novembre 2007 |
| Date de la dernière version | – |
| Source(s) | Mise à jour de sécurité Gentoo du 21 novembre 2007 Mise à jour de sécurité d'Ubuntu du 27 novembre 2007 |
| 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 ;
- déni de service ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

PCRE versions antérieures à la version 7.3.

3 Description

La bibliothèque PCRE (*Perl Compatible Regular Expressions*) est un ensemble de fonctions permettant d'utiliser des expressions régulières construites sémantiquement et syntaxiquement de la même manière que les expressions régulières de Perl.

De multiples vulnérabilités ont été découvertes dans la bibliothèque PCRE. L'exploitation de ces vulnérabilités permet à un utilisateur malintentionné d'effectuer diverses actions telles que le déni de service, l'accès à des données sensibles, ou l'exécution de code arbitraire.

4 Solution

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

5 Documentation

- Bulletin de sécurité Debian DSA 1399 du 06 novembre 2007 :
<http://www.debian.org/security/2007/dsa-1399>
- Bulletin de sécurité Gentoo GLSA-200711-30 du 21 novembre 2007 :
<http://www.gentoo.org/security/en/glsa/glsa-200711-30.xml>
- Bulletin de sécurité Ubuntu USN-547-1 du 27 novembre 2007 :
<http://www.ubuntulinux.org/usn/usn-547-1>
- Référence CVE CVE-2006-7227 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-7227>
- Référence CVE CVE-2006-7228 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-7228>
- Référence CVE CVE-2006-7230 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-7230>
- Référence CVE CVE-2007-1659 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1659>
- Référence CVE CVE-2007-1660 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1660>
- Référence CVE CVE-2007-1661 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1661>
- Référence CVE CVE-2007-1662 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1662>
- Référence CVE CVE-2007-4766 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4766>
- Référence CVE CVE-2007-4767 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4767>
- Référence CVE CVE-2007-4768 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4768>

Gestion détaillée du document

30 novembre 2007 version initiale.