Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 mars 2006
N° CERTA-2005-AVI-336-005

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du moteur d'expressions régulières PCRE

Gestion du document

Référence	CERTA-2005-AVI-336-005
Titre	Vulnérabilité du moteur d'expressions régulières PCRE
Date de la première version	07 septembre 2005
Date de la dernière version	10 mars 2006
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 ;
- exécution de code arbitraire ;
- exploitation à distance selon l'application utilisant la bibliothèque PCRE.

2 Systèmes affectés

Tout système utilisant la bibliothèque PCRE, qui est disponible pour Unix/MacOSX et Windows. De plus, de nombreux projets utilisent cette bibliothèque - en l'incluant éventuellement nativement - : les serveurs de messagerie `Exim` et `Postfix`, le serveur web `Apache`, la bibliothèque de KDE `kdelibs`, les outils d'analyse réseau `nmap`, `amap` et `ethereal`, l'analyseur de journaux de serveur web `analog`, les langages de script `Python` et `PHP`, le tableur `Gnumeric`,...

3 Résumé

Une vulnérabilité a été identifiée dans la gestion de l'allocation mémoire. Un utilisateur mal intentionné pourrait s'en servir pour provoquer un déni de service, voire exécuter du code arbitraire.

4 Description

PCRE (« Perl Compatible Regular Expressions ») est une bibliothèque de gestion des expressions régulières (motifs pour la recherche de textes) compatible avec la syntaxe présente dans `Perl`.

Dans le cas du serveur web `Apache`, l'interprétation des fichiers `.htaccess`, qui peuvent être placés dans tout répertoire de l'arborescence et en particulier les pages personnelles, est concernée.

5 Solution

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

Les services corrigés où liés dynamiquement à une bibliothèque mise à jour doivent être relancés (`Apache`, `Exim`, `Postfix`,...)

6 Documentation

- Site internet de la bibliothèque PCRE :
  http://www.pcre.org
- Mandriva Linux :
  - Bulletin de sécurité Mandriva MDKSA-2005:151 du 25 août 2005 (PCRE) :
    http://www.mandriva.com/security/advisories?name=MDKSA-2005:151
  - Bulletin de sécurité Mandriva MDKSA-2005:152 du 25 août 2005 (PHP) :
    http://www.mandriva.com/security/advisories?name=MDKSA-2005:152
  - Bulletin de sécurité Mandriva MDKSA-2005:153 du 26 août 2005 (Gnumeric) :
    http://www.mandriva.com/security/advisories?name=MDKSA-2005:153
  - Bulletin de sécurité Mandriva MDKSA-2005:154 du 26 août 2005 (Python) :
    http://www.mandriva.com/security/advisories?name=MDKSA-2005:154
  - Bulletin de sécurité Mandriva MDKSA-2005:155 du 29 août 2005 (Apache2) :
    http://www.mandriva.com/security/advisories?name=MDKSA-2005:155
- Debian Linux :
  - Bulletin de sécurité Debian DSA-800 du 02 septembre 2005 (PCRE) :
    http://www.debian.org/security/2005/dsa-800
  - Bulletin de sécurité Debian DSA-817 du 22 septembre 2005 (Python) :
    http://www.debian.org/security/2005/dsa-817
  - Bulletin de sécurité Debian DSA-819 du 23 septembre 2005 (Python) :
    http://www.debian.org/security/2005/dsa-819
  - Bulletin de sécurité Debian DSA-821 du 28 septembre 2005 (Python) :
    http://www.debian.org/security/2005/dsa-821
- SUSE Linux :
  - Bulletin de sécurité SUSE SuSE-SA:2005:048 du 30 août 2005 (PCRE) :
    http://www.novell.com/linux/security/advisories/2005_48_pcre.html
  - Bulletin de sécurité SUSE SuSE-SA:2005:049 du 30 août 2005 (PHP) :
    http://www.novell.com/linux/security/advisories/2005_49_php.html
  - Bulletin de sécurité SUSE SuSE-SA:2005:051 du 05 septembre 2005 (PHP) :
    http://www.novell.com/linux/security/advisories/2005_51_php.html
  - Bulletin de sécurité SUSE SuSE-SA:2005:051 du 12 septembre 2005 (Apache2) :
    http://www.novell.com/linux/security/advisories/2005_51_apache2.html
- Linux Fedora :
  - Mise à jour de sécurité pour Fedora Core 3 du 24 août 2005 :
    http://www.securityfocus.com/advisories/9121
  - Mise à jour de sécurité pour Fedora Core 4 du 24 août 2005 :
    http://www.securityfocus.com/advisories/9120

- Gentoo Linux :
  - Bulletin de sécurité Gentoo GLSA-200508-27 du 25 août 2005 (PCRE) : http://www.gentoo.org/security/en/glsa/glsa-200508-17.xml
  - Bulletin de sécurité Gentoo GLSA-200509-02 du 03 septembre 2005 (Gnumeric) : http://www.gentoo.org/security/en/glsa/glsa-200509-02.xml
  - Bulletin de sécurité Gentoo GLSA-200509-08 du 12 septembre 2005 (Python) : http://www.gentoo.org/security/en/glsa/glsa-200509-08.xml
  - Bulletin de sécurité Gentoo GLSA-200509-12 du 19 septembre 2005 (Apache) : http://www.gentoo.org/security/en/glsa/glsa-200509-12.xml
  - Bulletin de sécurité Gentoo GLSA-200509-19 du 27 septembre 2005 (PHP) : http://www.gentoo.org/security/en/glsa/glsa-200509-19.xml
- Bulletin de sécurité FreeBSD pour PCRE du 26 août 2005 : http://www.vuxml.org/freebsd/pkg-pcre.html
- Bulletin de sécurité OpenBSD pour PCRE du 22 août 2005 : http://www.vuxml.org/openbsd/pkg-pcre.html
- Vulnérabilité des sources `Apache` corrigées depuis 2.0.55-dev : http://httpd.apache.org/security/vulnerabilities_20.html
- Bulletin de sécurité RedHat RHSA-2005:761 du 08 septembre 2005 : http://rhn.redhat.com/errata/RHSA-2005-761.html
- Bulletin de sécurité RedHat RHSA-2006:0197 du 09 mars 2006 : http://rhn.redhat.com/errata/RHSA-2006-0197.html
- Référence CVE CAN-2005-2491 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2491

Gestion détaillée du document

07 septembre 2005 version initiale ;

14 septembre 2005 ajout de deux bulletins SuSE - Apache2 et un second PHP - et du bulletin Gentoo pour Python.

19 septembre 2005 ajout de la référence au bulletin de sécurité RedHat RHSA-2005:761.

22 septembre 2005 ajout de la référence au bulletin de sécurité Debian DSA-817.

23 septembre 2005 ajout de la référence au bulletin de sécurité Debian DSA-819.

28 septembre 2005 ajout de la référence au bulletin de sécurité Debian DSA-821.

10 mars 2006 ajout de la référence au bulletin de sécurité Gentoo GLSA-200509-12, Gentoo GLSA-200509-19 et RedHat RHSA-2006:0197.