

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Perl

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-2005-AVI-046>

Gestion du document

Référence	CERTA-2005-AVI-046-006
Titre	Vulnérabilité de Perl
Date de la première version	03 février 2005
Date de la dernière version	24 février 2005
Source(s)	Bulletin de sécurité FreeBSD du 02 février 2005
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

- Elévation de privilèges ;
- exécution de code arbitraire.

2 Systèmes affectés

Perl 5.8.6 et versions antérieures.

3 Description

Perl (Practical Extraction and Report Language) est un langage interprété de programmation.

Deux vulnérabilités dans l'interpréteur Perl permettent à un utilisateur mal intentionné d'élever ses privilèges (CAN-2005-0155) et de réaliser un débordement de mémoire (CAN-2005-0156) qui peut conduire à l'exécution de code arbitraire sur la plate-forme vulnérable.

4 Solution

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

5 Documentation

- Site Internet de Perl :
<http://www.perl.com>
- Bulletin de sécurité RedHat RHSA-2005:105 du 07 février 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-105.html>
- Bulletin de sécurité Mandrake MDKSA-2005:031 du 08 février 2005 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:031>
- Bulletin de sécurité FreeBSD du 02 février 2005 :
<http://www.vuxml.org/freebsd/>
- Mise à jour de sécurité du paquetage NetBSD perl58 :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/lang/perl58/README.html>
- Bulletin de sécurité Gentoo GLSA 200502-13 du 11 février 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200502-13.xml>
- Bulletin de sécurité RedHat RHSA-2005-103 du 15 février 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-103.html>
- Bulletin de sécurité SUSE-SR:2005:004 du 11 février 2005 :
http://www.novell.com/linux/security/advisories/2005_04_sr.html
- Bulletin de sécurité SGI 20050202-01-U du 09 février 2005 :
<ftp://patches.sgi.com/support/free/security/advisories/20050202-01-U.asc>
- Correctif de sécurité pour IBM AIX 5.2 et IBM AIX 5.3 :
<ftp://aix.software.ibm.com/aix/efixes/security/perl58x.tar>
- Référence CVE CAN-2005-0155 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0155>
- Référence CVE CAN-2005-0156 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0156>

Gestion détaillée du document

03 février 2005 version initiale.

08 février 2005 ajout de la référence au bulletin de sécurité RedHat RHSA-2005:105.

09 février 2005 ajout de la référence au bulletin de sécurité Mandrake MDKSA-2005:031.

14 février 2005 ajout des références aux bulletins de sécurité Gentoo GLSA 200502-13, SUSE SUSE-SR:2005:004 et SGI 20050202-01-U.

17 février 2005 ajout de la référence au bulletin de sécurité RedHat RHSA-2005:103.

24 février 2005 ajout de la référence au correctif de sécurité IBM.