



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 07 novembre 2007  
N° CERTA-2007-AVI-481

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-2007-AVI-481>

---

### Gestion du document

Référence	CERTA-2007-AVI-481
Titre	Vulnérabilité de Perl
Date de la première version	07 novembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Mandriva MDKSA-2007:207 du 05 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 à distance ;
- déni de service à distance.

## 2 Systèmes affectés

Perl 5.x versions antérieures à 5.9.5.

## 3 Résumé

Une vulnérabilité de Perl peut être exploitée par une personne malintentionnée distante pour effectuer un déni de service ou exécuter du code arbitraire.

## 4 Description

Une vulnérabilité de type débordement de mémoire a été identifiée dans Perl, plus précisément dans le traitement d'expressions régulières en *Unicode*. Ceci peut être exploité par une personne malintentionnée distante pour effectuer un déni de service voire exécuter du code arbitraire via une expression régulière spécialement construite.

## 5 Solution

La version de développement 5.9.5 corrige le problème. Se référer aux bulletins de sécurité des éditeurs pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité Debian DSA 1400-1 du 06 novembre 2007 :  
<http://www.debian.org/security/dsa-1400>
- Bulletin de sécurité Mandriva MDKSA-2007:207 du 05 novembre 2007 :  
<http://www.mandriva.com/en/security/advisories?name=MDKSA-2007:207>
- Bulletin de sécurité RedHat RHSA-2007:0966 du 05 novembre 2007 :  
<http://rhn.redhat.com/errata/RHSA-2007-0966.html>
- Bulletin de sécurité rPath 2007-0232-1 du 06 novembre 2007 :  
<http://lists.rpath.com/pipermail/security-announce/2007-November/000274.html>
- Bulletin de sécurité pour HP Tru64 Unix version 5.1B-4 du 21 février 2008 :  
[http://www.itrc.hp.com/service/patch/...I.do?patchid=perl\\_V51BB27-ES-20080207](http://www.itrc.hp.com/service/patch/...I.do?patchid=perl_V51BB27-ES-20080207)
- Bulletin de sécurité pour HP Tru64 Unix version 5.1B-3 du 21 février 2008 :  
<http://www.itrc.hp.com/service/patch/...hid=T64KIT1001399-V51BB26-ES-20071207>
- Bulletin de sécurité de SUN du 21 février 2008 :  
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-231524-1>
- Référence CVE CVE-2007-5116 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5116>

## Gestion détaillée du document

**07 novembre 2007** version initiale.