

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Apache

---

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-011>

---

### Gestion du document

Référence	CERTA-2008-AVI-011-002
Titre	Multiples vulnérabilités dans Apache
Date de la première version	09 janvier 2008
Date de la dernière version	14 février 2008
Source(s)	Bulletin de sécurité Apache
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

- Injection de code indirecte (*cross-site scripting*) ;
- déni de service à distance.

## 2 Systèmes affectés

Apache, versions 1.3.39 et antérieures, 2.0.61 et antérieures, 2.2.6 et antérieures.

## 3 Résumé

Plusieurs vulnérabilités dans le serveur HTTP Apache permettent à un utilisateur malveillant de réaliser de l'injection de code indirecte ou de provoquer un déni de service à distance.

## 4 Description

Une première vulnérabilité dans le module *mod\_imagemap* permet, quand ce module est activé et quand un fichier carte est public, de réaliser de l'injection de code indirecte.

Une vulnérabilité dans le module *mod\_status*, permet, quand ce module est activé et que la page d'état est publique, de réaliser de l'injection de code indirecte.

Une vulnérabilité dans le module *mod\_proxy\_balancer* permet, quand ce module est activé, de réaliser de l'injection de code indirecte contre un utilisateur autorisé.

Une deuxième vulnérabilité dans le module *mod\_proxy\_balancer* permet à un utilisateur autorisé malveillant de provoquer un arrêt inopiné du serveur par le biais d'une requête spécialement conçue.

## 5 Solution

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

## 6 Documentation

- Document du CERTA CERTA-2007-AVI-560 du 24 décembre 2007 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-560/index.html>
- Bulletins de sécurité Apache :  
[http://httpd.apache.org/security/vulnerabilities\\_22.html](http://httpd.apache.org/security/vulnerabilities_22.html)  
[http://httpd.apache.org/security/vulnerabilities\\_20.html](http://httpd.apache.org/security/vulnerabilities_20.html)  
[http://httpd.apache.org/security/vulnerabilities\\_13.html](http://httpd.apache.org/security/vulnerabilities_13.html)
- Bulletins de sécurité Red Hat du 15 janvier 2008 :  
<http://rhn.redhat.com/errata/RHSA-2008-0004.html>  
<http://rhn.redhat.com/errata/RHSA-2008-0005.html>  
<http://rhn.redhat.com/errata/RHSA-2008-0006.html>
- Bulletin de sécurité HP c01364714 du 11 février 2008 :  
<http://itrc.hp.com/service/cki/docDisplay.do?docId=c01364714>
- Référence CVE CVE-2007-5000 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5000>
- Référence CVE CVE-2007-6388 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6388>
- Référence CVE CVE-2007-6421 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6421>
- Référence CVE CVE-2007-6422 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6422>

## Gestion détaillée du document

**09 janvier 2008** version initiale.

**16 janvier 2008** ajout des références Red Hat.

**14 février 2008** ajout de la référence au bulletin de sécurité HP-UX.