



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 30 juin 2009  
N° CERTA-2009-AVI-257

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités de HP-UX Apache Web Server Suite

---

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-2009-AVI-257>

---

### Gestion du document

Référence	CERTA-2009-AVI-257
Titre	Multiples vulnérabilité de HP-UX Apache Web Server Suite
Date de la première version	30 juin 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité HP c01756421 du 29 juin 2009
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

- Apache Web Server Suite versions antérieures à v3.05 (HP-UX 11iv2 et 11iv3) ;
- Apache Web Server Suite versions antérieures à v2.25 (HP-UX 11iv1).

## 3 Résumé

Plusieurs vulnérabilités de *HP-UX Apache Web Server Suite* permettent de réaliser un déni de service à distance et d'exécuter du code arbitraire à distance.

## 4 Description

De multiples vulnérabilités liées au langage *PHP*, au serveur Web Apache et aux moteurs de servlet basés sur celui de *Tomcat* permettent à un individu distant de réaliser un déni de service ou d'exécuter du code arbitraire. Ces vulnérabilités ont été décrites dans les avis précédents du CERTA.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité HP c01756421 du 29 juin 2009 :  
<http://itrc.hp.com/service/cki/docDisplay.do?docId=c01756421>
- Avis CERTA-2007-AVI-339 du 08 novembre 2007 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-339>
- Avis CERTA-2008-AVI-011 du 09 janvier 2008 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-011>
- Avis CERTA-2008-AVI-225 du 02 mai 2008 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-225>
- Avis CERTA-2008-AVI-417 du 08 août 2008 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-417>
- Avis CERTA-2009-AVI-083 du 03 mars 2009 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-083>
- Référence CVE CVE-2007-4465 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4465>
- Référence CVE CVE-2008-0005 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0005>
- Référence CVE CVE-2008-0599 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0599>
- Référence CVE CVE-2008-2168 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2168>
- Référence CVE CVE-2008-2371 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2371>
- Référence CVE CVE-2008-2665 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2665>
- Référence CVE CVE-2008-2666 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2666>
- Référence CVE CVE-2008-2829 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2829>
- Référence CVE CVE-2008-3959 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3959>
- Référence CVE CVE-2008-3660 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3660>
- Référence CVE CVE-2008-5498 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5498>
- Référence CVE CVE-2008-5557 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5557>
- Référence CVE CVE-2008-5624 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5624>
- Référence CVE CVE-2008-5625 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5625>
- Référence CVE CVE-2008-5658 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5658>

## Gestion détaillée du document

30 juin 2009 version initiale.