



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 septembre 2009  
N° CERTA-2009-AVI-413

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans HP-UX

---

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-413>

---

### Gestion du document

Référence	CERTA-2009-AVI-413
Titre	Vulnérabilités dans HP-UX
Date de la première version	30 septembre 2009
Date de la dernière version	–
Source(s)	Bulletins de sécurité HP-UX du 21 septembre 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

- Déni de service à distance ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

- DNS Bind Server sous T0685G06^AAA, T0685G06^AAC, T0685H01^AAB et T0685H01^AAD ;
- Role-Based Access Control sous HP-UX B.11.23 et HP-UX B.11.31.

## 3 Résumé

Deux vulnérabilités découvertes dans HP-UX peuvent être exploitées afin de contourner la politique de sécurité ou pour provoquer un déni de service à distance.

## 4 Description

- Une vulnérabilité dans le serveur DNS Bind peut être exploitée par un utilisateur distant malintentionné afin de provoquer un déni de service à distance (CVE-2009-0696) ;

- une vulnérabilité dans le modèle de contrôle d'accès RBAC (*Role-Based Access Control*) sous HP-UX peut être exploitée afin de contourner la politique de sécurité et permettre à un utilisateur local d'obtenir un accès illégitime (CVE-2009-2692).

## 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 c01855358 du 21 septembre 2009 :  
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01855358>
- Bulletin de sécurité HP c01866178 du 21 septembre 2009 :  
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01866178>
- Référence CVE CVE-2009-0696 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0696>
- Référence CVE CVE-2009-2682 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2682>

## Gestion détaillée du document

**30 septembre 2009** version initiale.