

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Compromission possible de certificats sur HP HTTP Server

---

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-2004-AVI-091>

---

### Gestion du document

Référence	CERTA-2004-AVI-091
Titre	Compromission possible de certificats sur <i>HP HTTP Server</i>
Date de la première version	15 mars 2004
Date de la dernière version	–
Source(s)	Avis de sécurité HP SSRT4679
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

Compromission de certificats.

## 2 Systèmes affectés

*HP HTTP Server* versions 5.0 à 5.92 incluse.

## 3 Résumé

Un utilisateur anonyme distant peut compromettre le serveur de certificats «de confiance».

## 4 Description

*HP HTTP Server* est un composant de *HP Web-enabled Management Software*.

Par défaut, l'option «Accès Anonyme» (*Anonymous Access*) est désactivée sur ce logiciel. Si l'option «Accès Anonyme» est activée, un utilisateur distant mal intentionné peut se connecter anonymement sur le serveur de certificats de confiance et compromettre celui-ci.

## **5 Contournement provisoire**

Désactiver l'option «Accès Anonyme» si elle est activée.

## **6 Solution**

Installer la version 5.93 de *HP HTTP Server*.

Pour les utilisateurs de Windows, un correctif est disponible sur le site de HP :

<http://h18023.www1.hp.com/support/files/Server/us/download/20197.html>

Pour les autres plateformes, la version 5.93 de *HP HTTP Server* sera incluse dans les prochaines mises à jour de *HP Web-enabled Management Software*.

## **7 Documentation**

Pour les clients HP :

<http://itrc.hp.com>

## **Gestion détaillée du document**

**15 mars 2004** version initiale.