

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans HP Performance Manager

---

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-2010-AVI-220>

---

### Gestion du document

Référence	CERTA-2010-AVI-220
Titre	Multiples vulnérabilités dans HP Performance Manager
Date de la première version	20 mai 2010
Date de la dernière version	–
Source(s)	Bulletin de scurit HP #c02181353 du 17 mai 2010
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 ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données ;
- élévation de privilèges ;
- injection de code indirecte à distance.

## 2 Systèmes affectés

- HP Performance Manager v8.21 ;
- HP Performance Manager v8.20 ;
- HP Performance Manager v8.10.

## 3 Résumé

Plusieurs vulnérabilités découvertes dans HP Performance Manager permettent à un utilisateur distant malintentionné de provoquer un déni de service, de contourner la politique de sécurité, de porter atteinte à la confiden-

tialité et à l'intégrité des données, d'élever ses privilèges ou encore de réaliser une attaque par injection de code indirecte.

## 4 Description

De nombreuses vulnérabilités ont été corrigées dans HP Performance Manager. Elles peuvent être exploitées par une personne malveillante afin de :

- de provoquer un déni de service (CVE-2009-0033) ;
- de contourner la politique de sécurité (CVE-2008-5515, CVE-2009-2901) ;
- de porter atteinte à l'intégrité des données (CVE-2009-0783, CVE-2009-2693, CVE-2009-2902) ;
- de porter atteinte à la confidentialité des données (CVE-2009-0580, CVE-2009-0783) ;
- d'élever ses privilèges (CVE-2009-3548) ;
- de réaliser une attaque par injection de code indirecte (CVE-2009-0781) ;

## 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 #c02181353 du 17 mai 2010 :  
[http://itrc.hp.com/service/cki/docDisplay.do?docId=emr\\_na-c02181353](http://itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02181353)  
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02181353>
- Référence CVE CVE-2008-5515 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5515>
- Référence CVE CVE-2009-0033 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0033>
- Référence CVE CVE-2009-0580 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0580>
- Référence CVE CVE-2009-0781 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0781>
- Référence CVE CVE-2009-0783 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0783>
- Référence CVE CVE-2009-2693 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2693>
- Référence CVE CVE-2009-2901 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2901>
- Référence CVE CVE-2009-2902 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2902>
- Référence CVE CVE-2009-3548 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3548>

## Gestion détaillée du document

20 mai 2010 version initiale.