



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 02 juin 2004  
N° CERTA-2004-AVI-179

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de HP OpenView Select Access

---

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-179>

---

### Gestion du document

Référence	CERTA-2004-AVI-179
Titre	Vulnérabilité de HP OpenView Select Access
Date de la première version	02 juin 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité HP HPSBMA01045
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

Contournement des restrictions d'accès.

## 2 Systèmes affectés

Les versions suivantes du produit HP OpenView Select Access sont affectées :

- 5.0 Patch 4 ;
- 5.1 Patch 1 ;
- 5.2 ;
- 6.0.

## 3 Résumé

Une vulnérabilité du composant *Select Access* du produit HP OpenView permet à un utilisateur mal intentionné de contourner les restrictions d'accès.

## **4 Description**

HP OpenView Select Access est une solution de gestion centralisée de la sécurité des applications web et des utilisateurs.

Une vulnérabilité dans le décodage des caractères *Unicode UTF-8* permet à un utilisateur mal intentionné d'accéder à des ressources non autorisées.

## **5 Solution**

Appliquer les correctifs proposés par HP et disponibles à l'adresse suivante :  
[http://support.openview.hp.com/cpe/select\\_access/patch\\_sa.jsp](http://support.openview.hp.com/cpe/select_access/patch_sa.jsp)

## **6 Documentation**

Site HP sur les solutions OpenView :  
<http://www.openview.hp.com>

## **Gestion détaillée du document**

**02 juin 2004** version initiale.