

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans HP OpenView Storage Data Protector

---

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-2011-AVI-260>

---

### Gestion du document

Référence	CERTA-2011-AVI-260
Titre	Multiples vulnérabilités dans HP OpenView Storage Data Protector
Date de la première version	27 avril 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité HP c02781143 du 25 avril 2011
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.

## 2 Systèmes affectés

– HP OpenView Storage Data Protector versions 6.00, 6.10 et 6.11 pour Windows, Linux et Solaris.

## 3 Résumé

Plusieurs vulnérabilités ont été corrigées dans HP OpenView Storage Data Protector, qui permettent à un attaquant d'exécuter du code arbitraire à distance.

## 4 Description

Plusieurs vulnérabilités ont été corrigées dans HP OpenView Storage Data Protector :

– dans l'exécutable crs.exe la vérification des noms d'hôte, de domaine et d'utilisateur n'est pas correctement faite et peut conduire à l'exécution de code arbitraire via des requêtes TCP spécialement conçues ;

- le logiciel client ne vérifie pas correctement les arguments, fichiers et adresses associés à la commande EXEC\_CMD et un attaquant peut en profiter pour exécuter du code arbitraire à distance.

## **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 c02781143 du 25 avril 2011 :  
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02781143>
- Référence CVE CVE-2011-0921 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0921>
- Référence CVE CVE-2011-0922 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0922>
- Référence CVE CVE-2011-0923 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0923>
- Référence CVE CVE-2011-0924 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0924>

## **Gestion détaillée du document**

**27 avril 2011** version initiale.