Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 janvier 2012
N° CERTA-2012-AVI-022

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

**Objet : Vulnérabilités dans HP StorageWorks Modular Smart Array P2000 G3**

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-2012-AVI-022

## Gestion du document

| | |
|---|---|
| Référence | CERTA-2012-AVI-022 |
| Titre | Vulnérabilités dans HP StorageWorks Modular Smart Array P2000 G3 |
| Date de la première version | 17 janvier 2012 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité HP du 13 janvier 2012 |
| 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

- Atteinte à la confidentialité des données ;
- exécution de code arbitraire à distance.

## 2 Systèmes affectés

HP StorageWorks Modular Smart Array P2000 G3 avec une version du microgiciel (*firmware*) antérieure à TS230P008.

## 3 Résumé

Des vulnérabilités présentes dans le microgiciel (*firmware*) du HP StorageWorks Modular Smart Array P2000 G3 ont été corrigées. Ces vulnérabilités permettent à un utilisateur malintentionné de porter atteinte à la confidentialité des données et d'exécuter du code arbitraire à distance.

# 4 Description

Des vulnérabilités dans le microgiciel (*firmware*) du HP StorageWorks Modular Smart Array P2000 G3 permettent à un utilisateur malintentionné de porter atteinte à la confidentialité des données et d'exécuter du code arbitraire à distance :

- certaines entrées de l'interface Web ne sont pas correctement validées et exposent la solution à des attaques de type traversée de répertoires (*directory traversal*) ;
- un mot de passe par défaut peut-être utilisé pour exécuter des tâches avec les droits administrateur.

# 5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). La version TS230P008 du microgiciel (*firmware*) corrige le problème.

# 6 Documentation

- Bulletin de sécurité HP du 13 janvier 2012 :
  http://h20565.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03153338
- Référence CVE CVE-2011-4788 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4788

# Gestion détaillée du document

**17 janvier 2012** version initiale.