

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans HP StorageWorks

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-2009-AVI-163>

Gestion du document

Référence	CERTA-2009-AVI-163
Titre	Multiples vulnérabilités dans HP StorageWorks
Date de la première version	27 avril 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité HP c01707538 du 20 avril 2009
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 ;
- déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- HP StorageWorks Storage Mirroring versions antérieures à 5.1.1.1090.15.

3 Résumé

Plusieurs vulnérabilités de *HP StorageWorks Storage Mirroring* permettent à un individu malintentionné et distant d'exécuter du code arbitraire, de réaliser un déni de service et de contourner la politique de sécurité.

4 Description

Il existe plusieurs vulnérabilités dans *HP StorageWorks Storage Mirroring* :

- la première concerne un débordement de mémoire dans le module *Auto-Discovery*, un individu malintentionné et distant peut exécuter du code arbitraire à l'aide d'un paquet UDP construit de façon particulière ;

- la deuxième concerne la console de management (*Management Console*), un individu malintentionné et distant peut réaliser un déni de service à l'aide d'un paquet UDP contruit de façon particulière ;
- la dernière concerne une faiblesse de chiffrement présente dans le module d'authentification de *HP Storage-Works Storage Mirroring*, un individu malintentionné et distant peut contourner la politique de sécurité.

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 c01707538 du 20 avril 2009 :
<http://itrc.hp.com/service/cki/docDisplay.do?docId=c01707538>
- Référence CVE CVE-2009-0716 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0716>
- Référence CVE CVE-2009-0717 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0717>
- Référence CVE CVE-2009-0718 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0718>

Gestion détaillée du document

27 avril 2009 version initiale.