Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 novembre 2006
N° CERTA-2006-AVI-475

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans HP System Management Homepage

Gestion du document

Référence	CERTA-2006-AVI-475
Titre	Multiples vulnérabilités dans HP System Management Homepage
Date de la première version	07 novembre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité HP du 01 novembre 2006
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 ;
- `cross-site scripting` ;
- contournement de la politique de sécurité.

2 Systèmes affectés

HP System Management Homepage (SMH) versions antérieures à 2.1.5.

3 Résumé

Plusieurs vulnérabilités dans `HP System Management Homepage` permettent à une personne distante malintentionnée de contourner la politique de sécurité, de réaliser de l'injection de code indirecte (`cross-site scripting`) ou de réaliser un déni de service.

4 Description

Les versions Linux et Windows de HP System Management Homepage contiennent de multiples failles dans les composants PHP :

- des vulnérabilités dans les fonctions PHP parse_str(), extract() et import_request_variables() permettent de contourner de la politique de sécurité ;
- une vulnérabilité dans la gestion des entrées de la fonction PHP phpinfo() permet de réaliser de l'injection de code indirecte (cross-site scripting) ;
- une vulnérabilité de type integer overflow dans l'utilisation des bibliothèques PCRE peut conduire à un déni de service.

5 Solution

La version 2.1.5 de HP System Management Homepage corrige les vulnérabilités.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

Bulletin de sécurité HP c00786522 du 01 novembre 2006 :
http://itrc.hp.com/service/cki/docDisplay.do?docId=c00786522

Gestion détaillée du document

07 novembre 2006 version initiale.