Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 février 2008
N° CERTA-2007-AVI-435-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans HP System Management Homepage

Gestion du document

Référence	CERTA-2007-AVI-435-001
Titre	Vulnérabilité dans HP System Management Homepage
Date de la première version	10 octobre 2007
Date de la dernière version	14 février 2008
Source(s)	Bulletins de sécurité HP c01183265 et c01183597 du 03 octobre 2007
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 indirecte à distance (*Cross Site Scripting* ou *XSS*).

2 Systèmes affectés

- HP System Management Homepage (SMH) versions antérieures à 2.1.10 (pour GNU/Linux et Microsoft Windows) ;
- HP System Management Homepage (SMH) sur HP-UX versions B.11.11, B.11.23 et B.11.31.

3 Résumé

Une vulnérabilité de `HP System Management Homepage` (`SMH`) permet l'exécution de code indirecte à distance.

4 Description

Le manque de contrôle du contenu d'un argument envoyé à `HP System Management Homepage` (`SMH`) permet à un individu malveillant de réaliser de l'injection de code indirecte à distance (*Cross Site Scripting* ou *XSS*).

5 Solution

La version 2.1.10-186 pour GNU/Linux et Microsoft Windows corrige le problème. Les correctifs PHSS_36869, PHSS_36870 et PHSS_36871 pour HP-UX corrigent le problème. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité HP c01183265 du 03 octobre 2007 :
  http://itrc.hp.com/service/cki/docDisplay.do?docId=c01183265
- Bulletin de sécurité HP c01183597 du 03 octobre 2007 :
  http://itrc.hp.com/service/cki/docDisplay.do?docId=c01183597
- Référence CVE CVE-2007-5302 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5302

Gestion détaillée du document

10 octobre 2007 version initiale.
14 février 2008 ajout de la référence CVE.