

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans HP SOA Registry Fondation

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-2010-AVI-148>

Gestion du document

Référence	CERTA-2010-AVI-148
Titre	Multiples vulnérabilités dans HP SOA Registry Fondation
Date de la première version	31 mars 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité HPSBMA02490 du 30 mars 2010
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

- Contournement de la politique de sécurité ;
- élévation de privilèges ;
- injection de code indirecte à distance.

2 Systèmes affectés

HP SOA Registry Fondation versions 6.64 et antérieures.

3 Résumé

Plusieurs vulnérabilités présentes dans HP SOA Registry Fondation permettent à un utilisateur distant de contourner la politique de sécurité du système, d'élever ses privilèges et de conduire des attaques de type injection de code indirecte.

4 Description

Plusieurs vulnérabilités non détaillées par l'éditeur sont présentes dans HP SOA Registry Fondation :

- la première permet à un utilisateur distant malintentionné d'obtenir un accès frauduleux à certaines données du système ;
- la seconde permet à un utilisateur distant malintentionné d'élever ses privilèges ;
- la dernière est relative à un manque de contrôle dans les entrées passées à certaines pages HTML et permet à un utilisateur distant de conduire des attaques de type injection de code indirecte.

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 HPBMA02490 du 30 mars 2010 :
<http://itrc.hp.com/service/cki/docDisplay.do?docId=HPBMA02490>
- Référence CVE CVE-2010-0448 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0448>
- Référence CVE CVE-2010-0449 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0449>
- Référence CVE CVE-2010-0450 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0450>

Gestion détaillée du document

31 mars 2010 version initiale.