

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Avaya Aura System Manager

---

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-739>

---

### Gestion du document

Référence	CERTA-2012-AVI-739
Titre	Multiples vulnérabilités dans Avaya Aura System Manager
Date de la première version	14 décembre 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Avaya ASA-2011-122 du 03 février 2011 Bulletin de sécurité Avaya ASA-2011-122 du 28 avril 2011
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

## 1 Risques

- Exécution de code arbitraire à distance ;
- déni de service à distance.

## 2 Systèmes affectés

- Avaya Aura System Manager version 5.2
- Avaya Aura System Manager branche 6.0.x
- Avaya Aura System Manager branche 6.1.x
- Avaya Aura System Manager branche 6.2.x

## 3 Résumé

De multiples vulnérabilités ont été corrigées dans *Avaya Aura System Manager*. Certaines d'entre elles permettent à un attaquant d'exécuter du code arbitraire à distance.

## **4 Solution**

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## **5 Documentation**

- Bulletin de sécurité Avaya ASA-2011-122 du 03 février 2011 :  
<https://downloads.avaya.com/css/P8/documents/100126851>
- Bulletin de sécurité Avaya ASA-2011-122 du 28 avril 2011 :  
<https://downloads.avaya.com/css/P8/documents/100134336>

## **Gestion détaillée du document**

**14 décembre 2012** version initiale.