

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Avaya Aura Session 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-616>

Gestion du document

Référence	CERTA-2012-AVI-616
Titre	Vulnérabilité dans Avaya Aura Session Manager
Date de la première version	02 novembre 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Avaya ASA-2012-344 du 22 août 2012
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.

2 Systèmes affectés

- Avaya IQ avec la branche 3.x
- Avaya Aura Session Manager version 6.2.1 et version 6.2.2
- Avaya Voice Portal version 5.1.3

3 Résumé

Une vulnérabilité a été corrigée dans *Avaya Aura Session Manager*. Elle permet à un attaquant local de provoquer un déni de service au moyen d'une application spécialement conçue. Elle concerne les versions antérieures à la version 3.2.24 du noyau *Linux*.

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-2012-344 du 22 août 2012 :
<https://downloads.avaya.com/css/P8/documents/100165733>
- Référence CVE CVE-2012-3375 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3375>

Gestion détaillée du document

02 novembre 2012 version initiale.