Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 décembre 2012
N° CERTA-2012-AVI-734

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les produits Avaya

Gestion du document

Référence	CERTA-2012-AVI-734
Titre	Vulnérabilité dans les produits Avaya
Date de la première version	13 décembre 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Avaya 100167371 du 10 décembre 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

Exécution de code arbitraire.

2 Systèmes affectés

- Avaya Aura Application Enablement Services versions 5.x et 6.x
- Avaya Aura Application Server 5300 versions 2.x et 3.x
- Avaya IQ version 5.x
- Avaya Aura Communication Manager version 6.x
- Avaya Communication Server 1000 versions 6.x et 7.x
- Avaya Aura Conferencing Standard Edition version 6.x
- Avaya IP Office Application Server version 8.x
- Avaya Aura Messaging version 6.x
- Avaya one-X Client Enablement Services version 6.x
- Avaya Aura Presence Services version 6.x
- Avaya Proactive Contact version 5.x
- Avaya Aura Session Manager versions 1.x, 5.x, 6.1.x, 6.2 à 6.2.2
- Avaya Aura System Manager versions 5.x, 6.1.x et 6.2.x

- Avaya Aura System Platform versions 1.x et 6.x
- Avaya Aura Communication Manager Utility Services version 6.x
- Avaya Voice Portal version 5.x

3 Résumé

Une vulnérabilité a été corrigée dans les produits *Avaya*. Elle concerne des débordements d'entiers dans les fonctions *strtod()*, *strtof()* et *strtold()* pouvant mener à des débordement de tampon en mémoire. Un utilisateur malintentionné peut ainsi 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 100167371 du 10 décembre 2012 :
  https://downloads.avaya.com/css/P8/documents/100167371
- Référence CVE CVE-2012-3480 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3480

Gestion détaillée du document

13 décembre 2012 version initiale.