

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Avaya Interaction Center

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-070>

Gestion du document

Référence	CERTA-2012-AVI-070
Titre	Vulnérabilité dans Avaya Interaction Center
Date de la première version	09 février 2012
Date de la dernière version	–
Source(s)	Notes de mise à jour Avaya Interaction Center du 09 janvier 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 à distance.

2 Systèmes affectés

Avaya Interaction Center, vulnérabilité confirmée dans la version 7.2.3, d'autres versions peuvent néanmoins être affectées.

3 Résumé

Une vulnérabilité dans *Avaya Interaction Center* permet à une personne malintentionnée d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité est présente dans *Avaya Interaction Center*.

La vulnérabilité se trouve dans le service *Avaya Interaction Center ORB* et est due à une erreur de validation de données en entrée lors du traitement de certains paquets. Une personne malintentionnée peut exploiter cette

vulnérabilité en envoyant des paquets spécialement conçus sur le port 9001, provoquant un dépassement de tampon sur la pile (*stack-based buffer overflow*).

L'exploitation réussie permet d'exécuter du code arbitraire à distance.

5 Solution

Effectuer une mise à jour vers la version 7.2.4 ou supérieure.

6 Documentation

- Notes de mise à jour Avaya Interaction Center du 09 janvier 2012 :
<https://support.avaya.com/css/P8/documents/100154707>

Gestion détaillée du document

09 février 2012 version initiale.