

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Avaya

---

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-2007-AVI-475>

---

### Gestion du document

Référence	CERTA-2007-AVI-475
Titre	Vulnérabilité dans Avaya
Date de la première version	05 novembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Avaya n415 du 01 novembre 2007
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 à distance.

## 2 Systèmes affectés

- Avaya Messaging Storage Server 3.1 ;
- Avaya Message Networking 3.1.

## 3 Résumé

Une vulnérabilité dans des produits Avaya permet à un individu malveillant d'effectuer un déni de service à distance.

## 4 Description

Une vulnérabilité dans des produits Avaya permet à un individu malveillant d'effectuer un déni de service à distance via l'envoi de requêtes spécifiques par l'interface web d'administration.

## **5 Solution**

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

## **6 Documentation**

- Bulletin de sécurité Avaya n 415 du 01 novembre 2007  
<http://support.avaya.com/elmodocs2/security/ASA-2007-415.htm>

## **Gestion détaillée du document**

**05 novembre 2007** version initiale.