

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Avaya Modular Messaging

---

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-2005-AVI-511>

---

### Gestion du document

Référence	CERTA-2005-AVI-511
Titre	Vulnérabilité dans Avaya Modular Messaging POP3
Date de la première version	30 décembre 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco
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 Modular Messaging 2.x.

## 3 Résumé

Une vulnérabilité présente dans le serveur POP3 de Avaya Modular Messaging peut être exploitée par un utilisateur mal intentionné pour réaliser un déni de service.

## 4 Description

Une vulnérabilité présente dans le service POP3 de Avaya Modular Messaging peut être exploitée par un utilisateur mal intentionné, via des paquets malicieusement construits, pour réaliser un déni de service sur le serveur vulnérable.

## **5 Solution**

Appliquer le correctif disponible sur le site de l'éditeur (cf. section documentation).

## **6 Documentation**

- Site internet d'avaya :  
<http://www.avaya.com>
- Bulletin de sécurité Avaya :  
<http://support.avaya.com/elmodocs2/PSN/PSN599u.pdf>

## **Gestion détaillée du document**

**30 décembre 2005** version initiale.