

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Asterisk

---

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-2009-AVI-129>

---

### Gestion du document

Référence	CERTA-2009-AVI-129
Titre	Vulnérabilité dans Asterisk
Date de la première version	06 avril 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité du projet Asterisk AST-2009-003 du 02 avril 2009
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

Atteinte à la confidentialité des données.

## 2 Systèmes affectés

- Asterisk Open Source 1.x ;
- Asterik Business Edition ;
- Asterik Appliance s800i.

## 3 Résumé

Une vulnérabilité dans Asterisk permet à un utilisateur malveillant d'obtenir des informations sensibles.

## 4 Description

Quand Asterisk est utilisé avec l'option *alwaysauthreject*, la réponse SIP diffère selon que l'utilisateur existe ou n'existe pas. Cette différence est exploitable par un utilisateur malveillant pour obtenir la liste des utilisateurs valides.

## **5 Solution**

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

## **6 Documentation**

- Bulletin de sécurité du projet Asterisk AST-2009-003 du 02 avril 2009 :  
<http://www.asterisk.org/node/48582>
- Référence CVE CVE-2008-3903 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3903>

## **Gestion détaillée du document**

**06 avril 2009** version initiale.