

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-2008-AVI-006>

---

### Gestion du document

Référence	CERTA-2008-AVI-006
Titre	Vulnérabilité dans Asterisk
Date de la première version	08 janvier 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité du projet Asterisk AST-2008-001 du 02 janvier 2008
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 ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

- Asterisk Open Source, pour les versions de la branche 1.4.x antérieures à 1.4.17 ;
- Asterisk Business Edition, pour les versions de la branche C.x.x antérieures à C.1.0-beta8 ;
- AsteriskNOW pour les versions antérieures à beta7 ;
- Asterisk Appliance Developer Kit pour les versions antérieures à Asterisk 1.4 revision 95946 ;
- s800i (Asterisk Appliance) pour les versions de la branche 1.0.x antérieures à 1.0.3.4.

## 3 Résumé

Une vulnérabilité a été identifiée dans Asterisk. Elle pourrait être exploitée à distance par le biais de trames spécialement construites, afin de perturber le service.

## 4 Description

Une vulnérabilité a été identifiée dans Asterisk. L'application ne manipulerait pas correctement les trames signalant la fermeture d'une session d'appel SIP (BYE) et un transfert (en-tête "Also"). Celui-ci n'est normalement plus utilisé, et a été remplacé par la méthode `Refer`.

Cette vulnérabilité pourrait être exploitée à distance par le biais de trames spécialement construites afin de perturber le service Asterisk.

## 5 Solution

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

## 6 Documentation

- Annonce de sécurité du projet Asterisk AST-2008-001 du 02 janvier 2008 :  
<http://downloads.digium.com/pub/security/AST-2008-001.html>
- Référence CVE CVE-2008-0095 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0095>
- RFC 3515, "The Session Initiation Protocol (SIP) Refer Method" :  
<http://www.ietf.org/rfc/rfc3115.txt>

## Gestion détaillée du document

**08 janvier 2008** version initiale.