

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités 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-2011-AVI-371>

---

### Gestion du document

Référence	CERTA-2011-AVI-371
Titre	Vulnérabilités dans Asterisk
Date de la première version	29 juin 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Asterisk AST-2011-008 du 20 juin 2011 Bulletin de sécurité Asterisk AST-2011-009 du 23 juin 2011 Bulletin de sécurité Asterisk AST-2011-010 du 22 juin 2011
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

- Asterisk Open Source 1.4.x ;
- Asterisk Open Source 1.6.x ;
- Asterisk Open Source 1.8.x ;
- Asterisk Business Edition C.3.

## 3 Résumé

Plusieurs vulnérabilités présentes dans *Asterisk* permettent à un utilisateur distant malintentionné, authentifié ou non sur le système, de provoquer un déni de service.

## 4 Description

Plusieurs vulnérabilités ont été découvertes dans différentes versions d'*Asterisk*.

La vulnérabilité dénommée AST-2011-008 permet à une personne malintentionnée de causer un déni de service à distance grâce à l'envoi de requêtes SIP contenant un octet nul. Cette vulnérabilité affecte les versions 1.6.0.x, 1.6.1.x, 1.6.2.x et 1.8.x de *Asterisk Open Source*.

La faille AST-2011-009 concerne le pilote de canal SIP. Le problème survient lors de la réception d'un paquet SIP contenant un en-tête *Contact* malformé. Elle touche le produit *Asterisk Open Source* dans ses versions 1.8.x.

La dernière vulnérabilité corrigée, AST-2011-010, résoud un problème présent dans le pilote de canal IAX2. Lors de l'utilisation de ce protocole, le message transmis contient une adresse mémoire à laquelle le poste récepteur va tenter d'accéder, provoquant ainsi un arrêt brutal de l'application. Cette vulnérabilité touche les versions 1.4.x inférieures à 1.4.37, 1.6.2.x inférieures à 1.6.2.15 et 1.8.x de *Asterisk Open Source* ainsi que les versions C.3.x inférieures à C.3.6 de *Asterisk Business Edition*.

## 5 Solution

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

## 6 Documentation

- Référence CVE CVE-2011-2529 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2529>
- Référence CVE CVE-2011-2535 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2535>
- Bulletin de sécurité Asterisk AST-2011-008 :  
<http://downloads.asterisk.org/pub/security/AST-2011-008.html>
- Bulletin de sécurité Asterisk AST-2011-009 :  
<http://downloads.asterisk.org/pub/security/AST-2011-009.html>
- Bulletin de sécurité Asterisk AST-2011-010 :  
<http://downloads.asterisk.org/pub/security/AST-2011-010.html>

## Gestion détaillée du document

29 juin 2011 version initiale.