

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples 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-098>

---

### Gestion du document

|                             |   |
|-----------------------------|---|
| Référence                   | CERTA-2011-AVI-098-001                                    |
| Titre                       | Multiples vulnérabilités dans Asterisk                    |
| Date de la première version | 22 février 2011   |
| Date de la dernière version | 04 mai 2011   |
| Source(s)                   | Avis de sécurité Asterisk AST-2011-002 du 21 février 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

Exécution de code arbitraire à distance.

## 2 Systèmes affectés

- Asterisk Open Source 1.4.x ;
- Asterisk Open Source 1.6.x ;
- Asterisk Business Edition C.x.x ;
- AsteriskNOW 1.5 ;
- s800i 1.2.x.

## 3 Résumé

Plusieurs vulnérabilités dans Asterisk permettent l'exécution de code arbitraire à distance.

## 4 Description

De multiples débordements de mémoire dans Asterisk permettent à une personne malintentionnée d'exécuter du code arbitraire en envoyant des paquets UDPTL spécialement conçus.

## 5 Solution

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

## 6 Documentation

- Avis de sécurité Asterisk AST-2011-002 du 21 février 2011 :  
<http://downloads.asterisk.org/pub/security/AST-2011-002.html>
- Bulletin de sécurité Debian DSA-2225 du 25 avril 2011 :  
<http://www.debian.org/security/2011/dsa-2225>
- Référence CVE CVE-2011-1147 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1147>

## Gestion détaillée du document

**22 février 2011** version initiale.

**04 mai 2011** ajout de la référence CVE CVE-2011-1147 et du bulletin de sécurité Debian.