

Affaire suivie par :  
CERT-FR

## AVIS DU CERT-FR

**Objet : Multiples vulnérabilités dans Asterisk**

### Gestion du document

Référence	CERTFR-2016-AVI-302
Titre	Multiples vulnérabilités dans Asterisk
Date de la première version	09 septembre 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Asterisk AST-2016-006 du 08 septembre 2016 Bulletin de sécurité Asterisk AST-2016-007 du 08 septembre 2016
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(s)

- déni de service à distance

### 2 - Systèmes affectés

- Asterisk Open Source antérieures à 11.23.1
- Asterisk Open Source versions 13.X antérieures à 13.11.1
- Certified Asterisk versions antérieures à 11.6-cert15
- Certified Asterisk versions 13.8 antérieures à 13.8-cert3

### 3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Asterisk*. Elles permettent à un attaquant de provoquer un déni de service à distance.

### 4 - Solution

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

## 5 - Documentation

- Bulletin de sécurité Asterisk AST-2016-006 du 08 septembre 2016  
<http://downloads.asterisk.org/pub/security/AST-2016-006.html>
- Bulletin de sécurité Asterisk AST-2016-007 du 08 septembre 2016  
<http://downloads.asterisk.org/pub/security/AST-2016-007.html>

## Gestion détaillée du document

**09 septembre 2016** version initiale.

---

Conditions d'utilisation de ce document : <http://cert.ssi.gouv.fr/cert-fr/apropos.html>

Dernière version de ce document : <http://cert.ssi.gouv.fr/site/CERTFR-2016-AVI-302>

---