Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

**S . G . D . S . N**
*Agence nationale de la sécurité des systèmes d'information*
*CERTA*

Paris, le 19 mars 2008
N° CERTA-2008-AVI-150

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

## Objet : Multiples vulnérabilités dans Asterisk



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2008-AVI-150 |
| Titre | Multiples vulnérabilités dans Asterisk |
| Date de la première version | 19 mars 2008 |
| Date de la dernière version | – |
| Source(s) | Bulletins de sécurité Asterisk publiés le 18 mars 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 ;
- atteinte à l'intégrité des données.

## 2 Systèmes affectés

- Asterisk Open Source 1.2.x pour les versions antérieures à 1.2.27 ;
- Asterisk Open Source 1.4.x pour les versions antérieures à 1.4.18.1 et 1.4.19-rc3 ;
- Asterisk Open Source 1.6.x pour les versions antérieures à 1.6.0-beta6 ;
- Asterisk Business Edition B.x.x pour les versions antérieures à B.2.5.1 ;
- Asterisk Business Edition C.x.x pour les versions antérieures à C.1.6.1 ;
- AsteriskNOW 1.0.x pour les versions antérieures à 1.0.2 ;
- Asterisk Appliance Developer Kit (SVN) pour les versions antérieures à 1.4 revision 109386 ;
- s800i (Asterisk Appliance) 1.1.x pour les versions antérieures à 1.1.0.2.

# 3 Résumé

Plusieurs vulnérabilités ont été identifiées dans le gestionnaire de téléphonie sur IP Asterisk. Celles-ci peuvent être exploitées afin de perturber le service, lancer des appels à l'insu des utilisateurs ou écrire dans des zones de mémoire arbitraires.

# 4 Description

Plusieurs vulnérabilités ont été identifiées dans le gestionnaire de téléphonie sur IP Asterisk :

- l'application ne manipulerait pas correctement certains contenus RTP, provoquant des écritures dans des zones arbitraires de la mémoire. Ces vulnérabilités peuvent être exploitées par le biais de toute requête SIP avec SDP (*Session Description Protocol*), comme `INVITE`.
- il serait possible de lancer des appels non authentifiés à cause d'un mauvais contrôle du champs `From` de l'en-tête SIP par le pilote de canal SIP. Il s'agit du contournement de l'option de configuration `allowguest`.
- le format de journalisation des messages n'est pas interprété correctement via l'interface `ast_verbose`.
- la génération des identifiants de session (*manager ID*) dans le serveur AsteriskGUI HTTP serait relativement prévisible.

Ces vulnérabilités peuvent donc être exploitées afin de perturber le service, lancer des appels à l'insu des utilisateurs ou écrire dans des zones de mémoire arbitraires.

# 5 Solution

Se référer aux bulletins du projet Asterisk pour l'obtention des correctifs (cf. section Documentation).

# 6 Documentation

- Bulletin de sécurité AST-2008-002 du projet Asterisk du 18 mars 2008 :
  http://downloads.digium.com/pub/security/AST-2008-002.html
- Bulletin de sécurité AST-2008-003 du projet Asterisk du 18 mars 2008 :
  http://downloads.digium.com/pub/security/AST-2008-003.html
- Bulletin de sécurité AST-2008-004 du projet Asterisk du 18 mars 2008 :
  http://downloads.digium.com/pub/security/AST-2008-004.html
- Bulletin de sécurité AST-2008-005 du projet Asterisk du 18 mars 2008 :
  http://downloads.digium.com/pub/security/AST-2008-005.html
- Référence CVE CVE-2008-1289 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1289
- Référence CVE CVE-2008-1332 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1332
- Référence CVE CVE-2008-1333 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1333
- Référence CVE CVE-2008-1390 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1390

# Gestion détaillée du document

**19 mars 2008** version initiale.