

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-2009-AVI-102>

Gestion du document

Référence	CERTA-2009-AVI-102
Titre	Vulnérabilité dans Asterisk
Date de la première version	18 mars 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Asterisk AST-2009-002 du 10 mars 2009
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, branche 1.4.x pour les versions 1.4.22, 1.4.23 et 1.4.23.1 (sans à la révision 174082) ;
- Asterisk Open Source, branche 1.6.0.x pour les versions antérieures à 1.6.0.6 (sans la révision 174085) ;
- Asterisk Open Source, branche 1.6.1.x pour les versions antérieures à 1.6.1.0-rc2 (sans la révision 174086) ;
- Asterisk Business Edition version C.2.3.

3 Résumé

Une vulnérabilité a été identifiée dans le serveur de téléphonie sur IP Asterisk. Un message SIP construit de manière particulière peut perturber le fonctionnement du service.

4 Description

Une vulnérabilité a été identifiée dans le serveur de téléphonie sur IP Asterisk. Elle concerne les fonctions `sip_uri_headers_cmp()` et `sip_uri_params_cmp()` qui ne manipulent pas correctement les informations contenues par certaines trames. Cette vulnérabilité fonctionne avec l'option de configuration `pedantic` activée. La vulnérabilité peut être exploitée par une personne distante pour perturber le fonctionnement du service de téléphonie.

5 Solution

Se référer au bulletin de sécurité AST-2009-002 pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Référence CVE CVE-2009-0871 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0871>
- Bulletin de sécurité AST-2009-002 de digium Asterisk du 10 mars 2009 :
<http://downloads.digium.com/pub/security/AST-2009-002.html>
- Site du projet Asterisk :
<http://www.asterisk.org/security>

Gestion détaillée du document

18 mars 2009 version initiale.