

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-2009-AVI-322>

Gestion du document

Référence	CERTA-2009-AVI-322
Titre	Multiples vulnérabilités dans Asterisk
Date de la première version	11 août 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Asterisk AST-2009-005 du 10 août 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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Asterisk Open Source, série 1.2.x pour les versions antérieures à 1.2.34 ;
- Asterisk Open Source, série 1.4.x pour les versions antérieures à 1.4.26.1 ;
- Asterisk Open Source, série 1.6.0.x pour les versions antérieures à 1.6.0.12 ;
- Asterisk Open Source, série 1.6.1.x pour les versions antérieures à 1.6.1.4 ;
- Asterisk Business Edition, série A.x.x ;
- Asterisk Business Edition, série B.x.x pour les versions antérieures à B.2.5.9 ;
- Asterisk Business Edition, série C.2.x pour les versions antérieures à C.2.4.1 ;
- Asterisk Business Edition, série C.3.x pour les versions antérieures à C.3.1 ;
- boîtiers s800i, série 1.2.x pour les versions antérieures à 1.3.0.3.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans la plateforme de téléphonie (PBX) Asterisk. L'exploitation de ces dernières peut provoquer un dysfonctionnement du service.

4 Description

Plusieurs vulnérabilités ont été identifiées dans la plateforme de téléphonie (PBX) Asterisk. Elles concernent l'usage incorrect de la fonction `C sscanf` dans le code de l'application. Les données qui lui sont passées en entrée sont de longueur arbitraire et non contrôlée. Ce mauvais contrôle peut être exploité par une personne distante via des trames spécialement construites (Invite SIP par exemple) afin de perturber le service.

5 Solution

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

6 Documentation

- Bulletin de sécurité Asterisk AST-2009-005 du 10 août 2009 :
<http://downloads.asterisk.org/pub/security/AST-2009-005.html>
- Référence CVE CVE-2009-2726 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2726>

Gestion détaillée du document

11 août 2009 version initiale.