Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 septembre 2009
N° CERTA-2009-AVI-374

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Asterisk

Gestion du document

Référence	CERTA-2009-AVI-374
Titre	Vulnérabilité dans Asterisk
Date de la première version	09 septembre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Asterisk AST-2009-006 du 3 septembre 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

Contournement de la politique de sécurité.

2 Systèmes affectés

- Asterisk Open Source, série 1.2.x pour les versions antérieures à 1.2.35 ;
- Asterisk Open Source, série 1.4.x pour les versions antérieures à 1.4.26.2 ;
- Asterisk Open Source, série 1.6.0.x pour les versions antérieures à 1.6.0.15 ;
- Asterisk Open Source, série 1.6.1.x pour les versions antérieures à 1.6.1.6 ;
- Asterisk Business Edition, série B.x.x pour les versions antérieures à B.2.5.10 ;
- Asterisk Business Edition, série C.2.x pour les versions antérieures à C.2.4.3 ;
- Asterisk Business Edition, série C.3.x pour les versions antérieures à C.3.1.1 ;
- boîtiers s800i, série 1.3.x pour les versions antérieures à 1.3.0.3.

3 Résumé

Une vulnérabilité dans le protocole `IAX2` permettant l'établissement de sessions à distance non identifiées a été corrigée.

4 Description

Le protocole `IAX2` utilise des messages ayant comme identifiant de session un champ de taille fixe, le *numéro d'appel*. Ces messages ne demandant pas de confirmation (*ack*) une personne malveillante peut submerger la plate-forme en utilisant éventuellement des adresses IP usurpées, afin d'utiliser tous les *numéros d'appel* et empêcher l'identification de nouvelles sessions.

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-2009-006 du 3 septembre 2009 :
  http://downloads.asterisk.org/pub/security/AST-2009-006.html
- Référence CVE CVE-2009-2346 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2346

Gestion détaillée du document

09 septembre 2009 version initiale.