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 2012
N° CERTA-2012-AVI-153

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Asterisk

Gestion du document

Référence	CERTA-2012-AVI-153
Titre	Vulnérabilités dans Asterisk
Date de la première version	19 mars 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Asterisk AST-2012-002 du 14 mars 2012 Bulletin de sécurité Asterisk AST-2012-003 du 15 mars 2012
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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- Asterisk versions 1.4.X inférieures à 1.4.44 ;
- Asterisk versions 1.6.2.X inférieures à 1.6.2.23 ;
- Asterisk versions 1.8.X inférieures à 1.8.10.1 ;
- Asterisk versions 10.X inférieures à 10.2.1.

3 Résumé

Deux vulnérabilités ont été corrigées dans *Asterisk*. L'une d'entre elles permet l'exécution de code arbitraire à distance.

4 Description

Les versions 1.8.X et les versions 10.X sont vulnérables à de l'injection de code indirect à distance, par un attaquant anonyme.
Toutes les versions décrites ci-dessus sont également affectées par une vulnérabilité permettant, dans certaines configurations d'*Asterisk*, de fermer inopinément l'application à distance.

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-2012-002 du 14 mars 2012 :
  http://downloads.asterisk.org/pub/security/AST-2012-002.html
- Bulletin de sécurité Asterisk AST-2012-003 du 15 mars 2012 :
  http://downloads.asterisk.org/pub/security/AST-2012-003.html

Gestion détaillée du document

19 mars 2012 version initiale.