

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-2011-AVI-249>

Gestion du document

Référence	CERTA-2011-AVI-249-001
Titre	Multiples vulnérabilités dans Asterisk
Date de la première version	22 avril 2011
Date de la dernière version	04 mai 2011
Source(s)	Bulletins de sécurité AST-2011-005 et AST-2011-006 du 21 avril 2011
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 ;
- élévation de privilèges.

2 Systèmes affectés

- Asterisk 1.4.x ;
- Asterisk 1.6.1.x ;
- Asterisk 1.6.2.x ;
- Asterisk 1.8.x ;
- Asterisk Business Edition C.x.x.

3 Résumé

Deux vulnérabilités ont été découvertes dans *Asterisk* :

- Il est possible de provoquer un déni de service à distance ;
- un utilisateur authentifié sur la console d'administration peut exécuter du code arbitraire sur le système.

4 Description

Deux vulnérabilités ont été découvertes dans *Asterisk* :

- Une personne malveillante peut provoquer un déni de service en saturant le serveur au moyen d'un grand nombre de connexions TCP non authentifiées (Protocole Skinny, SIP sur TCP, sur le serveur HTTP ou sur l'interface d'administration) ;
- une erreur dans la console d'administration permet à un utilisateur authentifié de contourner des mesures de protection en place, et d'exécuter du code arbitraire sur le système.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).
Les versions 1.4.40.1, 1.6.1.25, 1.6.2.17.3, 1.8.3.3 et C.3.6.4 corrigent ces vulnérabilités.

6 Documentation

- Bulletin de sécurité Asterisk AST-2011-005 du 21 avril 2011 :
<http://downloads.asterisk.org/pub/security/AST-2011-005.html>
- Bulletin de sécurité Asterisk AST-2011-006 du 21 avril 2011 :
<http://downloads.asterisk.org/pub/security/AST-2011-006.html>
- Bulletin de sécurité Debian DSA-2225 du 25 avril 2011 :
<http://www.debian.org/security/2011/dsa-2225>
- Référence CVE CVE-2011-1507 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1507>
- Référence CVE CVE-2011-1599 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1599>

Gestion détaillée du document

22 avril 2011 version initiale.

04 mai 2011 ajout de la référence CVE CVE-2011-1599 et du bulletin de sécurité Debian.