

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-2011-AVI-023>

Gestion du document

Référence	CERTA-2011-AVI-023
Titre	Vulnérabilité dans Asterisk
Date de la première version	20 janvier 2011
Date de la dernière version	–
Source(s)	Bulletin de Sécurité Asterisk AST-2011-001 du 18 janvier 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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- Asterisk Open Source, versions antérieures à la version 1.4.38.1 ;
- Asterisk Open Source, versions antérieures à la version 1.4.39.1 ;
- Asterisk Open Source, versions antérieures à la version 1.6.1.21 ;
- Asterisk Open Source, versions antérieures à la version 1.6.2.15.1 ;
- Asterisk Open Source, versions antérieures à la version 1.6.2.16.1 ;
- Asterisk Open Source, versions antérieures à la version 1.8.1.2 ;
- Asterisk Open Source, versions antérieures à la version 1.8.2.1 ;
- Asterisk Business Edition, versions antérieures à la version C.3.6.2.

3 Résumé

Une vulnérabilité a été corrigée dans Asterisk Open Source et Business Edition. Elle permet à un utilisateur malintentionné d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité a été corrigée dans Asterisk Open Source et Business Edition. Elle permet, lorsque le serveur est configuré en mode « pedantic », à un utilisateur malintentionné et préalablement authentifié d'exécuter du code arbitraire à distance au moyen d'une requête SIP sortante spécialement conçue.

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-2011-001 du 18 janvier 2011 :
<http://downloads.asterisk.org/pub/security/AST-2011-001.html>
- Référence CVE CVE-2011-0495 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0495>

Gestion détaillée du document

20 janvier 2011 version initiale.