Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 24 novembre 2014
N° CERTFR-2014-AVI-493

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Asterisk

Gestion du document

Référence	CERTFR-2014-AVI-493
Titre	Multiples vulnérabilités dans Asterisk
Date de la première version	24 novembre 2014
Date de la dernière version	–
Source(s)	Bulletin de sécurité Asterisk du 20 novembre 2014 Bulletin de sécurité Asterisk du 20 novembre 2014 Bulletin de sécurité Asterisk du 20 novembre 2014 Bulletin de sécurité Asterisk du 20 novembre 2014 Bulletin de sécurité Asterisk du 20 novembre 2014 Bulletin de sécurité Asterisk du 20 novembre 2014 Bulletin de sécurité Asterisk du 20 novembre 2014
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(s)

- déni de service à distance
- contournement de la politique de sécurité
- élévation de privilèges

2 - Systèmes affectés

- Asterisk Open Source versions antérieures à 1.8.32.1
- Asterisk Open Source versions antérieures à 11.14.1
- Asterisk Open Source versions antérieures à 12.7.1
- Asterisk Open Source versions antérieures à 13.0.1
- Certified Asterisk versions antérieures à 1.8.28-cert3
- Certified Asterisk versions antérieures à 11.6-cert8

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Asterisk*. Elles permettent à un attaquant de provoquer un déni de service à distance, un contournement de la politique de sécurité et une élévation de privilèges.

4 - Solution

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

5 - Documentation

- Bulletin de sécurité Asterisk du 20 novembre 2014
  http://downloads.asterisk.org/pub/security/AST-2014-018.pdf
- Bulletin de sécurité Asterisk du 20 novembre 2014
  http://downloads.asterisk.org/pub/security/AST-2014-017.pdf
- Bulletin de sécurité Asterisk du 20 novembre 2014
  http://downloads.asterisk.org/pub/security/AST-2014-016.pdf
- Bulletin de sécurité Asterisk du 20 novembre 2014
  http://downloads.asterisk.org/pub/security/AST-2014-015.pdf
- Bulletin de sécurité Asterisk du 20 novembre 2014
  http://downloads.asterisk.org/pub/security/AST-2014-014.pdf
- Bulletin de sécurité Asterisk du 20 novembre 2014
  http://downloads.asterisk.org/pub/security/AST-2014-013.pdf
- Bulletin de sécurité Asterisk du 20 novembre 2014
  http://downloads.asterisk.org/pub/security/AST-2014-012.pdf
- Référence CVE CVE-2014-8412
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8412
- Référence CVE CVE-2014-8413
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8413
- Référence CVE CVE-2014-8414
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8414
- Référence CVE CVE-2014-8415
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8415
- Référence CVE CVE-2014-8416
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8416
- Référence CVE CVE-2014-8417
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8417
- Référence CVE CVE-2014-8418
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8418

Gestion détaillée du document

24 novembre 2014 version initiale.