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 17 septembre 2014
N° CERTFR-2014-AVI-390

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Wireshark

Gestion du document

Référence	CERTFR-2014-AVI-390
Titre	Multiples vulnérabilités dans Wireshark
Date de la première version	17 septembre 2014
Date de la dernière version	–
Source(s)	Bulletin de sécurité Wireshark wnpa-sec-2014-12 du 16 septembre 2014 Bulletin de sécurité Wireshark wnpa-sec-2014-13 du 16 septembre 2014 Bulletin de sécurité Wireshark wnpa-sec-2014-14 du 16 septembre 2014 Bulletin de sécurité Wireshark wnpa-sec-2014-15 du 16 septembre 2014 Bulletin de sécurité Wireshark wnpa-sec-2014-16 du 16 septembre 2014 Bulletin de sécurité Wireshark wnpa-sec-2014-17 du 16 septembre 2014 Bulletin de sécurité Wireshark wnpa-sec-2014-18 du 16 septembre 2014 Bulletin de sécurité Wireshark wnpa-sec-2014-19 du 16 septembre 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

2 - Systèmes affectés

- Wireshark versions antérieures à 1.12.1
- Wireshark versions antérieures à 1.10.10

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Wireshark*. Elles permettent à un attaquant de provoquer un déni de service à distance.

4 - Solution

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

5 - Documentation

- Bulletin de sécurité Wireshark wnpa-sec-2014-12 du 16 septembre 2014
  https://www.wireshark.org/security/wnpa-sec-2014-12.html
- Bulletin de sécurité Wireshark wnpa-sec-2014-13 du 16 septembre 2014
  https://www.wireshark.org/security/wnpa-sec-2014-13.html
- Bulletin de sécurité Wireshark wnpa-sec-2014-14 du 16 septembre 2014
  https://www.wireshark.org/security/wnpa-sec-2014-14.html
- Bulletin de sécurité Wireshark wnpa-sec-2014-15 du 16 septembre 2014
  https://www.wireshark.org/security/wnpa-sec-2014-15.html
- Bulletin de sécurité Wireshark wnpa-sec-2014-16 du 16 septembre 2014
  https://www.wireshark.org/security/wnpa-sec-2014-16.html
- Bulletin de sécurité Wireshark wnpa-sec-2014-17 du 16 septembre 2014
  https://www.wireshark.org/security/wnpa-sec-2014-17.html
- Bulletin de sécurité Wireshark wnpa-sec-2014-18 du 16 septembre 2014
  https://www.wireshark.org/security/wnpa-sec-2014-18.html
- Bulletin de sécurité Wireshark wnpa-sec-2014-19 du 16 septembre 2014
  https://www.wireshark.org/security/wnpa-sec-2014-19.html
- Référence CVE CVE-2014-6421
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6421
- Référence CVE CVE-2014-6422
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6422
- Référence CVE CVE-2014-6423
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6423
- Référence CVE CVE-2014-6424
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6424
- Référence CVE CVE-2014-6425
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6425
- Référence CVE CVE-2014-6426
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6426
- Référence CVE CVE-2014-6427
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6427
- Référence CVE CVE-2014-6428
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6428
- Référence CVE CVE-2014-6429
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6429
- Référence CVE CVE-2014-6430
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6430
- Référence CVE CVE-2014-6431
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6431
- Référence CVE CVE-2014-6432
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6432

Gestion détaillée du document

17 septembre 2014 version initiale.