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 13 avril 2017
N° CERTFR-2017-AVI-114

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Wireshark

Gestion du document

Référence	CERTFR-2017-AVI-114
Titre	Multiples vulnérabilités dans Wireshark
Date de la première version	13 avril 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité Wireshark wnpa-sec-2017-21 du 12 avril 2017 Bulletin de sécurité Wireshark wnpa-sec-2017-20 du 12 avril 2017 Bulletin de sécurité Wireshark wnpa-sec-2017-19 du 12 avril 2017 Bulletin de sécurité Wireshark wnpa-sec-2017-18 du 12 avril 2017 Bulletin de sécurité Wireshark wnpa-sec-2017-17 du 12 avril 2017 Bulletin de sécurité Wireshark wnpa-sec-2017-16 du 12 avril 2017 Bulletin de sécurité Wireshark wnpa-sec-2017-15 du 12 avril 2017 Bulletin de sécurité Wireshark wnpa-sec-2017-14 du 12 avril 2017 Bulletin de sécurité Wireshark wnpa-sec-2017-13 du 12 avril 2017 Bulletin de sécurité Wireshark wnpa-sec-2017-12 du 12 avril 2017
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

2 - Systèmes affectés

– Wireshark versions 2.2.x antérieures à 2.2.6
– Wireshark versions 2.0.x antérieures à 2.0.12

3 - Résumé

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

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-2017-21 du 12 avril 2017
  https://www.wireshark.org/security/wnpa-sec-2017-21.html
- Bulletin de sécurité Wireshark wnpa-sec-2017-20 du 12 avril 2017
  https://www.wireshark.org/security/wnpa-sec-2017-20.html
- Bulletin de sécurité Wireshark wnpa-sec-2017-19 du 12 avril 2017
  https://www.wireshark.org/security/wnpa-sec-2017-19.html
- Bulletin de sécurité Wireshark wnpa-sec-2017-18 du 12 avril 2017
  https://www.wireshark.org/security/wnpa-sec-2017-18.html
- Bulletin de sécurité Wireshark wnpa-sec-2017-17 du 12 avril 2017
  https://www.wireshark.org/security/wnpa-sec-2017-17.html
- Bulletin de sécurité Wireshark wnpa-sec-2017-16 du 12 avril 2017
  https://www.wireshark.org/security/wnpa-sec-2017-16.html
- Bulletin de sécurité Wireshark wnpa-sec-2017-15 du 12 avril 2017
  https://www.wireshark.org/security/wnpa-sec-2017-15.html
- Bulletin de sécurité Wireshark wnpa-sec-2017-14 du 12 avril 2017
  https://www.wireshark.org/security/wnpa-sec-2017-14.html
- Bulletin de sécurité Wireshark wnpa-sec-2017-13 du 12 avril 2017
  https://www.wireshark.org/security/wnpa-sec-2017-13.html
- Bulletin de sécurité Wireshark wnpa-sec-2017-12 du 12 avril 2017
  https://www.wireshark.org/security/wnpa-sec-2017-12.html
- Référence CVE CVE-2017-7704
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7704
- Référence CVE CVE-2017-7701
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7701
- Référence CVE CVE-2017-7705
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7705
- Référence CVE CVE-2017-7700
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7700
- Référence CVE CVE-2017-7702
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7702
- Référence CVE CVE-2017-7703
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7703

Gestion détaillée du document

13 avril 2017 version initiale.