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 29 février 2016
N° CERTFR-2016-AVI-074

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Wireshark

Gestion du document

Référence	CERTFR-2016-AVI-074
Titre	Multiples vulnérabilités dans Wireshark
Date de la première version	29 février 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Wireshark wnpa-sec-2016-01 du 26 février 2016 Bulletin de sécurité Wireshark wnpa-sec-2016-02 du 26 février 2016 Bulletin de sécurité Wireshark wnpa-sec-2016-03 du 26 février 2016 Bulletin de sécurité Wireshark wnpa-sec-2016-04 du 26 février 2016 Bulletin de sécurité Wireshark wnpa-sec-2016-05 du 26 février 2016 Bulletin de sécurité Wireshark wnpa-sec-2016-06 du 26 février 2016 Bulletin de sécurité Wireshark wnpa-sec-2016-07 du 26 février 2016 Bulletin de sécurité Wireshark wnpa-sec-2016-08 du 26 février 2016 Bulletin de sécurité Wireshark wnpa-sec-2016-09 du 26 février 2016 Bulletin de sécurité Wireshark wnpa-sec-2016-10 du 26 février 2016 Bulletin de sécurité Wireshark wnpa-sec-2016-11 du 26 février 2016 Bulletin de sécurité Wireshark wnpa-sec-2016-12 du 26 février 2016 Bulletin de sécurité Wireshark wnpa-sec-2016-13 du 26 février 2016 Bulletin de sécurité Wireshark wnpa-sec-2016-14 du 26 février 2016 Bulletin de sécurité Wireshark wnpa-sec-2016-15 du 26 février 2016 Bulletin de sécurité Wireshark wnpa-sec-2016-16 du 26 février 2016 Bulletin de sécurité Wireshark wnpa-sec-2016-17 du 26 février 2016 Bulletin de sécurité Wireshark wnpa-sec-2016-18 du 26 février 2016
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 1.12.x antérieures à 1.12.10

– Wireshark versions 2.0.x antérieures à 2.0.2

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-2016-01 du 26 février 2016
https://www.wireshark.org/security/wnpa-sec-2016-01.html
– Bulletin de sécurité Wireshark wnpa-sec-2016-02 du 26 février 2016
https://www.wireshark.org/security/wnpa-sec-2016-02.html
– Bulletin de sécurité Wireshark wnpa-sec-2016-03 du 26 février 2016
https://www.wireshark.org/security/wnpa-sec-2016-03.html
– Bulletin de sécurité Wireshark wnpa-sec-2016-04 du 26 février 2016
https://www.wireshark.org/security/wnpa-sec-2016-04.html
– Bulletin de sécurité Wireshark wnpa-sec-2016-05 du 26 février 2016
https://www.wireshark.org/security/wnpa-sec-2016-05.html
– Bulletin de sécurité Wireshark wnpa-sec-2016-06 du 26 février 2016
https://www.wireshark.org/security/wnpa-sec-2016-06.html
– Bulletin de sécurité Wireshark wnpa-sec-2016-07 du 26 février 2016
https://www.wireshark.org/security/wnpa-sec-2016-07.html
– Bulletin de sécurité Wireshark wnpa-sec-2016-08 du 26 février 2016
https://www.wireshark.org/security/wnpa-sec-2016-08.html
– Bulletin de sécurité Wireshark wnpa-sec-2016-09 du 26 février 2016
https://www.wireshark.org/security/wnpa-sec-2016-09.html
– Bulletin de sécurité Wireshark wnpa-sec-2016-10 du 26 février 2016
https://www.wireshark.org/security/wnpa-sec-2016-10.html
– Bulletin de sécurité Wireshark wnpa-sec-2016-11 du 26 février 2016
https://www.wireshark.org/security/wnpa-sec-2016-11.html
– Bulletin de sécurité Wireshark wnpa-sec-2016-12 du 26 février 2016
https://www.wireshark.org/security/wnpa-sec-2016-12.html
– Bulletin de sécurité Wireshark wnpa-sec-2016-13 du 26 février 2016
https://www.wireshark.org/security/wnpa-sec-2016-13.html
– Bulletin de sécurité Wireshark wnpa-sec-2016-14 du 26 février 2016
https://www.wireshark.org/security/wnpa-sec-2016-14.html
– Bulletin de sécurité Wireshark wnpa-sec-2016-15 du 26 février 2016
https://www.wireshark.org/security/wnpa-sec-2016-15.html
– Bulletin de sécurité Wireshark wnpa-sec-2016-16 du 26 février 2016
https://www.wireshark.org/security/wnpa-sec-2016-16.html
– Bulletin de sécurité Wireshark wnpa-sec-2016-17 du 26 février 2016
https://www.wireshark.org/security/wnpa-sec-2016-17.html
– Bulletin de sécurité Wireshark wnpa-sec-2016-18 du 26 février 2016
https://www.wireshark.org/security/wnpa-sec-2016-18.html
– Référence CVE CVE-2015-2529
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2529
– Référence CVE CVE-2016-2521
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2521

- Référence CVE CVE-2016-2522
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2522
- Référence CVE CVE-2016-2523
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2523
- Référence CVE CVE-2016-2524
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2524
- Référence CVE CVE-2016-2525
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2525
- Référence CVE CVE-2016-2526
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2526
- Référence CVE CVE-2016-2527
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2527
- Référence CVE CVE-2016-2528
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2528
- Référence CVE CVE-2016-2530
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2530
- Référence CVE CVE-2016-2531
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2531
- Référence CVE CVE-2016-2532
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2532

Gestion détaillée du document

29 février 2016 version initiale.