Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 30 juillet 2013
N° CERTA-2013-AVI-444

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Wireshark

Gestion du document

Référence	CERTA-2013-AVI-444
Titre	Multiples vulnérabilités dans Wireshark
Date de la première version	30 juillet 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité Wireshark wnpa-sec-2013-42 du 26 juillet 2013 Bulletin de sécurité Wireshark wnpa-sec-2013-43 du 26 juillet 2013 Bulletin de sécurité Wireshark wnpa-sec-2013-44 du 26 juillet 2013 Bulletin de sécurité Wireshark wnpa-sec-2013-45 du 26 juillet 2013 Bulletin de sécurité Wireshark wnpa-sec-2013-46 du 26 juillet 2013 Bulletin de sécurité Wireshark wnpa-sec-2013-47 du 26 juillet 2013 Bulletin de sécurité Wireshark wnpa-sec-2013-48 du 26 juillet 2013 Bulletin de sécurité Wireshark wnpa-sec-2013-49 du 26 juillet 2013 Bulletin de sécurité Wireshark wnpa-sec-2013-50 du 26 juillet 2013 Bulletin de sécurité Wireshark wnpa-sec-2013-51 du 26 juillet 2013 Bulletin de sécurité Wireshark wnpa-sec-2013-52 du 26 juillet 2013 Bulletin de sécurité Wireshark wnpa-sec-2013-53 du 26 juillet 2013
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

– Version antérieures à Wireshark 1.10.1
– version antérieures à Wireshark 1.8.9

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-2013-42 du 26 juillet 2013
  http://www.wireshark.org/security/wnpa-sec-2013-42.html
- Bulletin de sécurité Wireshark wnpa-sec-2013-43 du 26 juillet 2013
  http://www.wireshark.org/security/wnpa-sec-2013-43.html
- Bulletin de sécurité Wireshark wnpa-sec-2013-44 du 26 juillet 2013
  http://www.wireshark.org/security/wnpa-sec-2013-44.html
- Bulletin de sécurité Wireshark wnpa-sec-2013-45 du 26 juillet 2013
  http://www.wireshark.org/security/wnpa-sec-2013-45.html
- Bulletin de sécurité Wireshark wnpa-sec-2013-46 du 26 juillet 2013
  http://www.wireshark.org/security/wnpa-sec-2013-46.html
- Bulletin de sécurité Wireshark wnpa-sec-2013-47 du 26 juillet 2013
  http://www.wireshark.org/security/wnpa-sec-2013-47.html
- Bulletin de sécurité Wireshark wnpa-sec-2013-48 du 26 juillet 2013
  http://www.wireshark.org/security/wnpa-sec-2013-48.html
- Bulletin de sécurité Wireshark wnpa-sec-2013-49 du 26 juillet 2013
  http://www.wireshark.org/security/wnpa-sec-2013-49.html
- Bulletin de sécurité Wireshark wnpa-sec-2013-50 du 26 juillet 2013
  http://www.wireshark.org/security/wnpa-sec-2013-50.html
- Bulletin de sécurité Wireshark wnpa-sec-2013-51 du 26 juillet 2013
  http://www.wireshark.org/security/wnpa-sec-2013-51.html
- Bulletin de sécurité Wireshark wnpa-sec-2013-52 du 26 juillet 2013
  http://www.wireshark.org/security/wnpa-sec-2013-52.html
- Bulletin de sécurité Wireshark wnpa-sec-2013-53 du 26 juillet 2013
  http://www.wireshark.org/security/wnpa-sec-2013-53.html
- Référence CVE CVE-2013-4920
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4920
- Référence CVE CVE-2013-4921
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4921
- Référence CVE CVE-2013-4922
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4922
- Référence CVE CVE-2013-4923
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4923
- Référence CVE CVE-2013-4924
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4924
- Référence CVE CVE-2013-4925
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4925
- Référence CVE CVE-2013-4926
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4926
- Référence CVE CVE-2013-4927
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4927
- Référence CVE CVE-2013-4928
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4928

- Référence CVE CVE-2013-4929
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4929
- Référence CVE CVE-2013-4930
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4930
- Référence CVE CVE-2013-4931
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4931
- Référence CVE CVE-2013-4932
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4932
- Référence CVE CVE-2013-4933
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4933
- Référence CVE CVE-2013-4934
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4934
- Référence CVE CVE-2013-4935
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4935
- Référence CVE CVE-2013-4936
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4936

Gestion détaillée du document

30 juillet 2013 version initiale.