

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Wireshark

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-612>

Gestion du document

Référence	CERTA-2011-AVI-612
Titre	Multiples vulnérabilités dans Wireshark
Date de la première version	02 novembre 2011
Date de la dernière version	–
Source(s)	Bulletins de sécurité Wireshark du 01 novembre 2011
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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

Wireshark versions strictement inférieures à 1.6.3.

3 Résumé

Plusieurs vulnérabilités ont été corrigées dans Wireshark, qui peuvent être exploitées à distance pour causer un déni de service ou exécuter du code arbitraire.

4 Description

Trois vulnérabilités ont été corrigées dans Wireshark. Un attaquant distant peut provoquer l'arrêt inopiné du logiciel en envoyant des trames spécialement conçues, ou en incitant un utilisateur à ouvrir un fichier de traces réseau malveillant. L'une de ces vulnérabilités est de type dépassement de tampon (CVE-2011-4102), une autre

est due à une variable non initialisée (CVE-2011-4100), la troisième est due à un déréférencement de pointeur (CVE-2011-4101). L'exécution de code à distance n'est pas exclue.

5 Solution

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

6 Documentation

- Bulletin de sécurité Wireshark wnpa-sec-2011-17 du 01 novembre 2011 :
<http://www.wireshark.org/security/wnpa-sec-2011-17.html>
- Bulletin de sécurité Wireshark wnpa-sec-2011-18 du 01 novembre 2011 :
<http://www.wireshark.org/security/wnpa-sec-2011-18.html>
- Bulletin de sécurité Wireshark wnpa-sec-2011-19 du 01 novembre 2011 :
<http://www.wireshark.org/security/wnpa-sec-2011-19.html>
- Référence CVE CVE-2011-4100 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4100>
- Référence CVE CVE-2011-4101 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4101>
- Référence CVE CVE-2011-4102 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4102>

Gestion détaillée du document

02 novembre 2011 version initiale.