

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : 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-2012-AVI-020>

Gestion du document

Référence	CERTA-2012-AVI-020
Titre	Vulnérabilités dans Wireshark
Date de la première version	16 janvier 2012
Date de la dernière version	–
Sources	Bulletins de sécurité Wireshark du 10 janvier 2012
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

Contournement de la politique de sécurité.

2 Systèmes affectés

Wireshark 1.4.x et 1.6.x.

3 Résumé

Plusieurs vulnérabilités affectent Wireshark et permettent de contourner la politique de sécurité.

4 Description

Plusieurs vulnérabilités affectent Wireshark :

- des analyseurs de formats ne vérifient pas les tailles des champs dans plusieurs formats de fichiers de capture. Ce défaut permet à un attaquant de provoquer l'arrêt inopiné de Wireshark ;
- une erreur de traitement de pointeurs nuls permet à un attaquant de provoquer l'arrêt inopiné de Wireshark ;
- l'analyseur RLC est sujet à un débordement de mémoire.

5 Solution

Les versions 1.4.11 et 1.6.5 de Wireshark résolvent ces problèmes.

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

6 Documentation

- Bulletin de sécurité Wireshark wnpa-sec-2012-01 du 10 janvier 2012 :
<http://www.wireshark.org/security/wnpa-sec-2012-01.html>
- Bulletin de sécurité Wireshark wnpa-sec-2012-02 du 10 janvier 2012 :
<http://www.wireshark.org/security/wnpa-sec-2012-02.html>
- Bulletin de sécurité Wireshark wnpa-sec-2012-03 du 10 janvier 2012 :
<http://www.wireshark.org/security/wnpa-sec-2012-03.html>

Gestion détaillée du document

16 janvier 2012 version initiale.