

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-2010-AVI-560>

Gestion du document

Référence	CERTA-2010-AVI-560
Titre	Vulnérabilités dans Wireshark
Date de la première version	23 novembre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Wireshark wnpa-sec-2010-13 du 18 novembre 2010 Bulletin de sécurité Wireshark wnpa-sec-2010-14 du 18 novembre 2010
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

Déni de service à distance.

2 Systèmes affectés

- Wireshark versions 1.2.0 à 1.2.12 ;
- Wireshark versions 1.4.0 à 1.4.1.

3 Résumé

Deux vulnérabilités dans le logiciel Wireshark permettent à un attaquant de provoquer un déni de service à distance.

4 Description

Deux vulnérabilités dans le logiciel Wireshark permettent à un attaquant de provoquer un arrêt inopiné du programme en envoyant des paquets spécialement conçus ou bien en poussant un utilisateur à lire un fichier de traces particulier.

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-2010-13 du 18 novembre 2010 :
<http://www.wireshark.org/security/wnpa-sec-2010-13.html>
- Bulletin de sécurité Wireshark wmpa-sec-2010-14 du 18 novembre 2010 :
<http://www.wireshark.org/security/wnpa-sec-2010-14.html>
- Référence CVE CVE-2010-4300 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4300>
- Référence CVE CVE-2010-4301 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4301>

Gestion détaillée du document

23 novembre 2010 version initiale.