

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-200>

Gestion du document

Référence	CERTA-2010-AVI-200-001
Titre	Vulnérabilité dans Wireshark
Date de la première version	06 mai 2010
Date de la dernière version	11 juin 2010
Source(s)	Bulletins de sécurité Wireshark du 05 mai 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 1.0.12 et antérieures ;
- Wireshark versions 1.2.7 et antérieures.

3 Résumé

Une vulnérabilité dans Wireshark permet à un utilisateur distant de provoquer un déni de service.

4 Description

Une vulnérabilité relative à l'analyseur de protocole DOCSIS (Data Over Cable Service Interface Specifications) est présente dans Wireshark. Elle permet à un utilisateur distant de provoquer un déni de service de l'application vulnérable.

5 Solution

Les versions 1.0.13 et 1.2.8 corrigent le problème :

<http://www.wireshark.org/download.html>

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

6 Documentation

– Site de Wireshark :

<http://www.wireshark.org>

– Bulletins de sécurité Wireshark du 05 mai 2010 :

<http://www.wireshark.org/security/wnpa-sec-2010-03.html>

<http://www.wireshark.org/security/wnpa-sec-2010-04.html>

– Référence CVE CVE-2010-1455 :

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1455>

Gestion détaillée du document

06 mai 2010 version initiale.

11 juin 2010 ajout de la référence CVE.