

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Wireshark (Ethereal)

---

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-2006-AVI-373>

---

### Gestion du document

Référence	CERTA-2006-AVI-373-001
Titre	Multiples vulnérabilités dans Wireshark (Ethereal)
Date de la première version	25 août 2006
Date de la dernière version	08 septembre 2006
Source(s)	Bulletin de sécurité Wireshark wnpa-sec-2006-002 du 23 août 2006
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

- Les versions Ethereal/Wireshark antérieures à 0.99.3.

## 3 Résumé

Plusieurs vulnérabilités ont été identifiées dans Wireshark (Ethereal). Elles permettraient à une personne malveillante distante, de provoquer une perturbation du service ou d'exécuter des commandes arbitraires sur le système utilisant une version vulnérable.

## 4 Description

Ethereal est un logiciel de capture et d'analyse de trafic réseau. Le projet Ethereal a été interrompu, et son développement se poursuit maintenant sous le nom de Wireshark. Plusieurs vulnérabilités ont été identifiées dans

ce dernier :

- l'interpréteur de données au format protocolaire SCSI (Small Computer System Interface) n'effectuerait pas correctement sa tâche et pourrait être interrompu sous certaines conditions ;
- l'interpréteur du protocole DHCP pourrait provoquer une erreur dans la bibliothèque Glib et perturber le système vulnérable, au cours de la manipulation de certaines données ;
- la manipulation d'IPsec ESP entraînerait des erreurs lors du déchiffrement de certaines données ;
- des données respectant le protocole Q.2931 (utilisé pour la signalisation du RNIS à large bande B-ISDN) seraient manipulées de manière non correcte par l'interpréteur SSCOP. Cette vulnérabilité pourrait entraîner un débordement de mémoire.

Ces vulnérabilités peuvent être exploitées par une personne malveillante distante : il lui faut envoyer des paquets spécialement conçus à destination d'un système vulnérable pour provoquer une perturbation du service Wireshark (Ethereal) et d'exécuter des commandes arbitraires.

## 5 Solution

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

## 6 Documentation

- Site du projet Wireshark, succédant à Ethereal :  
<http://www.wireshark.org>
- Bulletin de sécurité Wireshark wnpa-sec-2006-002 du 23 août 2006 :  
<http://www.wireshark.org/security/wnpa-sec-2006-02.html>
- Mise à jour Wireshark pour la version 0.99.3 :  
<http://www.wireshark.org/docs/relnotes/wireshark-0.99.3.html>
- Référence CVE CVE-2006-4330 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4330>
- Référence CVE CVE-2006-4331 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4331>
- Référence CVE CVE-2006-4332 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4332>
- Référence CVE CVE-2006-4333 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4333>
- Bulletin de sécurité Debian dsa-1171-1 du 07 septembre 2006 :  
<http://www.debian.org/security/2006/dsa-1171>

## Gestion détaillée du document

**25 août 2006** version initiale.

**08 septembre 2006** ajout de la mise à jour Debian