

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de 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-2007-AVI-067>

Gestion du document

Référence	CERTA-2007-AVI-067
Titre	Multiples vulnérabilités de Wireshark (Ethereal)
Date de la première version	05 février 2007
Date de la dernière version	–
Source(s)	Annnonce des modifications pour Wireshark 0.99.5 du 01 février 2007
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

- Dénis de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Wireshark, pour les versions antérieures à 0.99.5.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans Wireshark (Ethereal). Elles permettraient à une personne malveillante distante, de provoquer une perturbation du service 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 au cours de l'année 2006, et son développement se poursuit actuellement sous le nom de Wireshark.

De multiples vulnérabilités ont été identifiées dans ce dernier. Parmi celles-ci, certaines concernent :

- le module d'analyse du protocole TCP : l'analyse de paquets fragmentés HTTP ne serait pas correctement effectuée, du à un problème de mise en œuvre dans le fichier `packet-tcp.c` ;
- le module d'analyse du protocole HTTP : cette vulnérabilité n'est pas documentée ;
- le module d'analyse protocolaire 802.11, pour les trames Wi-Fi ;
- le module d'analyse du protocole LLT (*Low Latency Transport*), utilisé pour les communications entre serveurs utilisant le logiciel VCS (pour *Veritas Cluster Server*).

Une personne malveillante pourrait construire un paquet exploitant l'une de ces vulnérabilités, afin de perturber le service Wireshark, qui capturerait et tenterait d'analyser cette trame.

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-2007-01` du 01 février 2007 :
<http://www.wireshark.org/security/wnpa-sec-2007-01.html>
- Annonce des correctifs de la version 0.99.5 de Wireshark :
<http://www.wireshark.org/docs/relnotes/wireshark-0.99.5.html>
- Référence CVE `CVE-2007-0456` :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0456>
- Référence CVE `CVE-2007-0457` :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0457>
- Référence CVE `CVE-2007-0458` :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0458>
- Référence CVE `CVE-2007-0459` :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0459>

Gestion détaillée du document

05 février 2007 version initiale.