Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S.G.D.S.N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 31 décembre 2007
N° CERTA-2007-AVI-559-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples 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-2007-AVI-559

Gestion du document

Référence	CERTA-2007-AVI-559-001
Titre	Multiples vulnérabilités dans Wireshark
Date de la première version	20 décembre 2007
Date de la dernière version	31 décembre 2007
Source(s)	Bulletin de sécurité Wireshark wnpa-sec-2007-03 du 18 décembre 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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

- Les versions de Wireshark et tshark antérieures à 0.99.7.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans l'outil d'analyse protocolaire Wireshark (prolongement de l'ancien projet Ethereal). Celles-ci peuvent être exploitées au moyen de trames spécialement construites et envoyées à distance, afin de perturber le service.

4 Description

Plusieurs vulnérabilités ont été identifiées dans l'outil d'analyse protocolaire Wireshark (prolongement de l'ancien projet Ethereal). Elles concernent notamment un ensemble de modules utilisés pour interpréter des protocoles ou des formats comme : `DNP`, `SSL`, `HTTP`, `PPP`, Bluetooth `SDP`, `IPv6`, `SMB`, etc.

Ces vulnérabilités peuvent être exploitées par une personne malveillante, au moyen de trames spécialement construites et envoyées à distance, afin de perturber le service, ou dans certaines conditions, d'exécuter du code arbitraire sur le système où le service est installé.

5 Solution

Se référer au bulletin de sécurité wnpa-sec-2007-03 du projet Wireshark pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site officiel du projet Wireshark :
  http://www.wireshark.org
- Bulletin de sécurité Wireshark wnpa-sec-2007-03 du 18 décembre 2007 :
  http://www.wireshark.org/security/wnpa-sec-2007-03.html
- Référence CVE CVE-2007-6111 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6111
- Référence CVE CVE-2007-6112 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6112
- Référence CVE CVE-2007-6113 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6113
- Référence CVE CVE-2007-6114 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6114
- Référence CVE CVE-2007-6115 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6115
- Référence CVE CVE-2007-6116 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6116
- Référence CVE CVE-2007-6117 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6117
- Référence CVE CVE-2007-6118 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6118
- Référence CVE CVE-2007-6119 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6119
- Référence CVE CVE-2007-6120 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6120
- Référence CVE CVE-2007-6121 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6121
- Référence CVE CVE-2007-6438 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6438
- Référence CVE CVE-2007-6439 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6439
- Référence CVE CVE-2007-6440 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6440
- Référence CVE CVE-2007-6441 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6441
- Référence CVE CVE-2007-6442 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6442
- Référence CVE CVE-2007-6443 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6443
- Référence CVE CVE-2007-6444 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6444
- Référence CVE CVE-2007-6445 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6445

- Référence CVE CVE-2007-6446 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6446
- Référence CVE CVE-2007-6447 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6447
- Référence CVE CVE-2007-6448 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6448
- Référence CVE CVE-2007-6449 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6449
- Référence CVE CVE-2007-6450 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6450
- Référence CVE CVE-2007-6451 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6451

Gestion détaillée du document

20 décembre 2007 version initiale.
31 décembre 2007 ajout de références CVE.