



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 octobre 2006
N° CERTA-2006-AVI-469

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-2006-AVI-469>

Gestion du document

Référence	CERTA-2006-AVI-469
Titre	Multiples vulnérabilités dans Wireshark
Date de la première version	27 octobre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Wireshark du 27 octobre 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

Wireshark (ou Ethereal) versions 0.99.3 et antérieures.

3 Résumé

De multiples vulnérabilités sont présentes dans Wireshark et permettent à un utilisateur distant malintentionné de provoquer un déni de service ou l'exécution de code arbitraire.

4 Description

Différents composants de Wireshark (anciennement Ethereal) comportent des vulnérabilités de type débordement de mémoire :

- l'analyseur de protocole HTTP (CVE-2006-5468) ;

- l'analyseur de protocole LDAP (CVE-2006-5740) ;
- l'analyseur de protocole XOT (CVE-2006-4805) ;
- l'analyseur de protocole WBXML (CVE-2006-5469) ;
- l'analyseur de format MIME Multipart (CVE-2006-i4574) ;
- l'analyseur de clefs WEP si le support de AirPcap est activé.

Toutes ces vulnérabilités permettent à un utilisateur distant malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire par le biais de paquets ou de trames construits de façon particulière.

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-2006-03 du 27 octobre 2006 :
<http://www.wireshark.org/security/wnpa-sec-2006-03.html>
- Référence CVE CVE-2006-5468 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5468>
- Référence CVE CVE-2006-5740 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5740>
- Référence CVE CVE-2006-4805 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4805>
- Référence CVE CVE-2006-5469 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5469>
- Référence CVE CVE-2006-4574 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4574>

Gestion détaillée du document

27 octobre 2006 version initiale.