Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 septembre 2006
N° CERTA-2006-AVI-301-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Ethereal/Wireshark

Gestion du document

Référence	CERTA-2006-AVI-301-002
Titre	Multiples vulnérabilités dans Ethereal/Wireshark
Date de la première version	19 juillet 2006
Date de la dernière version	28 septembre 2006
Source(s)	Bulletin de sécurité Wireshark du 17 juillet 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 de Wireshark (anciennement Ethereal) antérieures à la version 0.99.2.

3 Description

Wirehsark est un analyseur de trafic réseau qui succède à Ethereal. Plusieurs vulnérabilités ont été identifiées dans celui-ci ainsi que les versions Ethereal précédentes. Il s'agit pour la majorité de débordements de mémoire. Un utilisateur malveillant peut utiliser l'une d'entre elles pour construire un paquet spécial, qui provoquera le dysfonctionnement, voir l'interruption de l'application. Sous certaines conditions, une exécution de code à distance est également possible.

4 Solution

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

5 Documentation

- Site du projet Wireshark :
  http://www.wireshark.org
- Bulletin de sécurité Wireshark WNPA-SEC-2006-01 du 17 juillet 2006 :
  http://www.wireshark.org/security/wnpa-sec-2006-01.html
- Bulletin de sécurité Avaya ASA-2006-197 du 22 septembre 2006 :
  http://support.avaya.com/elmodocs2/security/ASA-2006-197.htm
- Bulletin de sécurité Red Hat RHSA-2006:0602 du 16 août 2006 :
  http://rhn.redhat.com/errata/RHSA-2006-0602.html
- Bulletin de sécurité SuSE SUSA-SA:2006:020 du 16 août 2006 :
  http://lists.suse.com/archive/suse-security-announce/2006-Aug/0006.html
- Bulletin de sécurité Debian DSA-1127 du 28 juillet 2006 :
  http://www.us.debian.org/security/dsa-1127/
- Bulletin de sécurité Gentoo GLSA-200607-09 du 25 juillet 2006 :
  http://www.gentoo.org/en/glsa/glsa-200607-09.xml
- Bulletin de sécurité Mandriva MDKSA-2006:128 du 18 juillet 2006 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2006:128
- Référence CVE CVE-2006-3627 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3627
- Référence CVE CVE-2006-3628 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3628
- Référence CVE CVE-2006-3629 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3629
- Référence CVE CVE-2006-3630 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3630
- Référence CVE CVE-2006-3631 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3631
- Référence CVE CVE-2006-3632 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3632

Gestion détaillée du document

19 juillet 2006 version initiale.
02 août 2006 ajout des références aux bulletins de sécurité Debian, Gentoo et Mandriva.
28 septembre 2006 ajout des références aux bulletins de sécurité Avaya, SuSE et Red Hat.