



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 juillet 2006
N° CERTA-2006-AVI-170-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le logiciel 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-170>

Gestion du document

Référence	CERTA-2006-AVI-170-003
Titre	Vulnérabilité dans le logiciel Ethereal
Date de la première version	26 avril 2006
Date de la dernière version	06 juillet 2006
Source(s)	Bulletin de mise à jour Ethereal
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

Ethereal versions 0.8.5 à 0.10.14.

3 Description

Plusieurs vulnérabilités ont été découvertes dans Ethereal. Ces vulnérabilités sont dues à différents types d'erreurs (erreurs aux limites, boucle infinie, ...) dans le gestionnaire de protocoles.

L'exploitation de ces vulnérabilités conduit à des effets divers parmi lesquels :

- déni de service de l'outil;
- déni de service de la machine;
- exécution de code arbitraire.

4 Solution

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

5 Documentation

- Pages de remontée de vulnérabilité d'Ethereal :
<http://www.ethereal.com/docs/release-notes/ethereal-0.99.0.html>
<http://www.ethereal.com/appnotes/enpa-sa-00023.html>
- Bulletin de sécurité Mandriva MDKSA-2006:077 du 25 avril 2006 :
<http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2006:077>
- Bulletin de sécurité Gentoo GLSA 200604-17 du 27 avril 2006 :
<http://www.gentoo.org/security/en/glsa/glsa-200604-17.xml>
- Bulletin de sécurité Debian DSA-1049 du 02 mai 2006 :
<http://www.debian.org/security/2006/dsa-1049>
- Bulletin de sécurité RedHat RHSA-2006:0420 du 03 mai 2006 :
<http://rhn.redhat.com/errata/RHSA-2006-0420.html>
- Bulletin de sécurité Suse SUSE-SR:2006:10 du 12 mai 2006 :
<http://lists.suse.com/archive/suse-security/announce/2006-May/0004.html>
- Bulletin de sécurité Avaya ASA-2006-128 du 30 juin 2006 :
<http://support.avaya.com/elmodocs2/security/ASA-2006-128.htm>
- Référence CVE CVE-2006-1932 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1932>
- Référence CVE CVE-2006-1933 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1933>
- Référence CVE CVE-2006-1934 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1934>
- Référence CVE CVE-2006-1935 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1935>
- Référence CVE CVE-2006-1936 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1936>
- Référence CVE CVE-2006-1937 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1937>
- Référence CVE CVE-2006-1938 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1938>
- Référence CVE CVE-2006-1939 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1939>
- Référence CVE CVE-2006-1940 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1940>

Gestion détaillée du document

26 avril 2006 version initiale.

04 mai 2006 ajout des références aux bulletins de sécurité Gentoo, Debian et RedHat.

16 mai 2006 ajout de la référence au bulletin de sécurité Suse.

06 juillet 2006 ajout de la référence au bulletin de sécurité Avaya.