

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités 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-2005-AVI-284>

Gestion du document

Référence	CERTA-2005-AVI-284-003
Titre	Multiples vulnérabilités dans le logiciel Ethereal
Date de la première version	28 juillet 2005
Date de la dernière version	10 octobre 2005
Source(s)	Bulletin de sécurité du logiciel 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

- Dénis de service ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

Ethereal versions 0.8.5 à 0.10.11 (incluses).

3 Description

Le logiciel Ethereal permet de capturer des trames réseau et d'effectuer de multiples actions sur celles-ci afin de faciliter leur analyse.

De multiples vulnérabilités ont été découvertes dans ce logiciel, permettant à un utilisateur mal intentionné de causer un déni de service ou d'exécuter du code arbitraire à distance.

Le premier problème concerne l'utilisation de la bibliothèque `zlib`, dont la vulnérabilité a été traitée dans l'avis du CERTA : CERTA-2005-AVI-276.

Les autres vulnérabilités sont induites par le traitement de certains protocoles. Ces vulnérabilités sont de type débordement de mémoire, chaîne de format, pointeur nul, et boucle infinie.

4 Solution

Mettre à jour Ethereal en version 0.10.12 :

<http://www.ethereal.com/download.html>

5 Documentation

- Site Internet d'Ethereal :
<http://www.ethereal.com>
- Bulletin de sécurité d'Ethereal :
<http://www.ethereal.com/appnotes/enpa-sa-00020.html>
- Avis du CERTA concernant la vulnérabilité de `zlib` :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-276/index.html>
- Bulletin de sécurité Gentoo GLSA-200507-27 du 28 juillet 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200507-27.xml>
- Bulletin de sécurité SuSE du 22 août 2005 :
http://www.novell.com/linux/security/advisories/2005_19_sr.html
- Bulletin de sécurité Red Hat RHSA-2005-687 du 11 août 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-687.html>
- Bulletin de sécurité Mandriva MDKSA-2005:131 du 05 août 2005 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:131>
- Bulletin de sécurité Avaya ASA-2005-185 du 29 août 2005 :
<http://support.avaya.com/elmodocs2/security/ASA-2005-185.pdf>
- Bulletin de sécurité FreeBSD pour ethereal, ethereal-lite, tethereal et tethereal-lite du 30 juillet 2005 :
<http://www.vuxml.org/freebsd/pkg-ethereal.html>
<http://www.vuxml.org/freebsd/pkg-ethereal-lite.html>
<http://www.vuxml.org/freebsd/pkg-tethereal.html>
<http://www.vuxml.org/freebsd/pkg-tethereal-lite.html>
- Bulletin de sécurité Debian DSA-853 du 09 octobre 2005 :
<http://www.debian.org/security/2005/dsa-853>
- Référence CVE CAN-2005-2360 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2360>
- Référence CVE CAN-2005-2361 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2361>
- Référence CVE CAN-2005-2362 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2362>
- Référence CVE CAN-2005-2363 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2363>
- Référence CVE CAN-2005-2364 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2364>
- Référence CVE CAN-2005-2365 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2365>
- Référence CVE CAN-2005-2366 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2366>
- Référence CVE CAN-2005-2367 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2367>

Gestion détaillée du document

28 juillet 2005 version initiale.

01 août 2005 ajout de la référence au bulletin de sécurité FreeBSD.

31 août 2005 ajout des références aux bulletins de sécurité SuSE, Red Hat, Mandriva et Avaya.

10 octobre 2005 ajout de la référence au bulletin de sécurité Debian et aux références CVE.