

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités d'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-178>

Gestion du document

Référence	CERTA-2005-AVI-178-003
Titre	Multiples vulnérabilités d'Ethereal
Date de la première version	27 mai 2005
Date de la dernière version	28 juin 2005
Source(s)	Bulletin de sécurité enpa-sa-00019 d'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 ;
- déni de service.

2 Systèmes affectés

Ethereal versions 0.10.10 et antérieures.

3 Résumé

Plusieurs vulnérabilités présentes dans Ethereal permettent à un utilisateur mal intentionné d'exécuter du code arbitraire ou d'effectuer un déni de service à distance.

4 Description

Ethereal est un renifleur réseau. Il permet l'analyse de données depuis le réseau ou à partir d'un fichier. De multiples vulnérabilités sont présentes dans les routines de dissection relatives à de nombreux types de flux (se référer au bulletin de sécurité de l'éditeur pour obtenir la liste complète).

Par le biais de paquets malicieusement construits, un utilisateur mal intentionné peut exploiter ces vulnérabilités afin d'effectuer un déni de service par arrêt brutal de l'application ou consommation excessive des ressources de la machine ou bien exécuter du code arbitraire sur le système vulnérable.

5 Solution

La version 0.10.11 d'Ethereal corrige ces vulnérabilités.

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

6 Documentation

- Site de l'éditeur :
<http://www.ethereal.com>
- Bulletin de sécurité d'Ethereal enpa-sa-00019 du 04 mai 2005 :
<http://www.ethereal.com/appnotes/enpa-sa-00019.html>
- Bulletin de sécurité de Gentoo GLSA 200505-03 du 06 mai 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200505-03.xml>
- Bulletin de sécurité de Mandrake MDKSA-2005:083 du 10 mai 2005 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:083>
- Bulletin de sécurité RedHat RHSA-2005:427 du 24 mai 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-427.html>
- Bulletin de sécurité SUSE SUSE-SR:2005:014 du 07 juin 2005 :
http://www.novell.com/linux/security/advisories/2005_14_sr.html
- Bulletin de sécurité Avaya ASA-2005-131 du 13 juin 2005 :
http://support.avaya.com/elmodocs2/security/ASA-2005-131_RHSA-2005-427.pdf
- Bulletin de sécurité FreeBSD du 28 juin 2005 :
<http://www.vuxml.org/freebsd/pkg-ethereal.html>
- Mise à jour de sécurité du paquetage NetBSD ethereal :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/net/ethereal/README.html>
- Référence CVE CAN-2005-1456 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1456>
- Référence CVE CAN-2005-1457 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1457>
- Référence CVE CAN-2005-1458 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1458>
- Référence CVE CAN-2005-1459 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1459>
- Référence CVE CAN-2005-1460 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1460>
- Référence CVE CAN-2005-1461 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1461>
- Référence CVE CAN-2005-1462 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1462>
- Référence CVE CAN-2005-0766 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1463>
- Référence CVE CAN-2005-1464 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1464>
- Référence CVE CAN-2005-1465 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1465>
- Référence CVE CAN-2005-1466 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1466>
- Référence CVE CAN-2005-1467 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1467>

- Référence CVE CAN-2005-1468 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1468>
- Référence CVE CAN-2005-1469 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1469>
- Référence CVE CAN-2005-1470 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1470>

Gestion détaillée du document

27 mai 2005 version initiale.

08 juin 2005 ajout référence au bulletin de sécurité SUSE.

17 juin 2005 ajout du bulletin de sécurité Avaya ASA-2005-131.

28 juin 2005 ajout références aux bulletins FreeBSD et NetBSD.