

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans 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-2004-AVI-099>

---

### Gestion du document

Référence	CERTA-2004-AVI-099-006
Titre	Vulnérabilités dans Ethereal
Date de la première version	24 mars 2004
Date de la dernière version	01 juin 2004
Source(s)	Avis de sécurité Ethereal enpa-sa-00013 du 22-03-2004
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

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

## 2 Systèmes affectés

Toutes les versions de Ethereal comprises entre les versions (incluses) 0.8.13 et 0.10.2.

## 3 Résumé

Plusieurs vulnérabilités dans Ethereal permettent à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire sur une plate-forme utilisant une version vulnérable d'Ethereal.

## 4 Description

Ethereal est un renifleur réseau. Il permet l'analyse de données depuis le réseau ou à partir d'un fichier. Un utilisateur mal intentionné, composant judicieusement un fichier destiné à être lu par Ethereal ou injectant un paquet malicieusement construit sur le réseau, peut exploiter une des vulnérabilités afin de réaliser un déni de service sur la plate-forme utilisant une version vulnérable d'Ethereal.

## 5 Solution

Mettre à jour Ethereal en version 0.10.3, soit par la compilation des sources, soit par l'application du correctif fourni par l'éditeur.

- Site internet de téléchargement de Ethereal :  
<http://www.ethereal.com/download>
- Bulletin de sécurité GLSA 200403-07 de Gentoo :  
<http://www.securityfocus.com/advisories/6482>
- Bulletin de sécurité MDKSA-2004:024 de Mandrake :  
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:024>
- Bulletin de sécurité RHSA-2004:136 de Red Hat :  
<http://rhn.redhat.com/errata/RHSA-2004-136.html>
- Bulletin de sécurité RHSA-2004:137 de RedHat :  
<http://rhn.redhat.com/errata/RHSA-2004-137.html>
- Bulletin de sécurité SUSE SuSE-SA:2004:012 du 14 mai 2004 :  
[http://www.suse.com/de/security/2004\\_12\\_mc.html](http://www.suse.com/de/security/2004_12_mc.html)
- Bulletin de sécurité Debian DSA-511 du 30 mai 2004 :  
<http://www.debian.org/security/2004/dsa-511>
- Bulletin de sécurité FreeBSD du 29 mars 2004 :  
<http://www.vuxml.org/freebsd>

## 6 Documentation

- Site internet de Ethereal :  
<http://www.ethereal.com>
- Avis de sécurité Ethereal enpa-sa-00013 du 22 mars 2004 :  
<http://www.ethereal.com/appnotes/enpa-sa-00013.html>
- Avis de sécurité e-matters du 23 mars 2004 :  
<http://security.e-matters.de/advisories/032004.html>
- Référence CVE CAN-2004-0176 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0176>
- Référence CVE CAN-2004-0365 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0365>
- Référence CVE CAN-2004-0367 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0367>

## Gestion détaillée du document

**24 mars 2004** version initiale.

**30 mars 2004** ajout référence au bulletin de sécurité de Gentoo.

**31 mars 2004** ajout référence au bulletin de sécurité de Mandrake.

**01 avril 2004** ajout référence au bulletin de sécurité de RedHat.

**13 mai 2004** ajout des bulletins de sécurité RedHat, FreeBSD et des références CVE CAN-2004-0365 et CAN-2004-0367.

**17 mai 2004** ajout de la référence au bulletin de sécurité SUSE.

**01 juin 2004** ajout de la référence au bulletin de sécurité Debian.