



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 14 janvier 2004  
N° CERTA-2004-AVI-003-001

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-003>

---

### Gestion du document

Référence	CERTA-2004-AVI-003-001
Titre	Vulnérabilités dans Ethereal
Date de la première version	08 janvier 2004
Date de la dernière version	14 janvier 2004
Source(s)	Bulletin de sécurité Ethereal enpa-sa-00012
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.

## 2 Systèmes affectés

Tous les systèmes avec Ethereal en version antérieure à la version 0.10.0.

## 3 Résumé

Deux vulnérabilités dans Ethereal permettent à un utilisateur mal intentionné de réaliser un déni de service 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 de ces vulnérabilités afin de réaliser un déni de service sur la plate-forme utilisant une version vulnérable d'Ethereal.

## 5 Contournement provisoire

Dans l'attente de l'application du correctif, désactiver les protocoles suivants : SMB et Q.931.

## 6 Solution

Installer la version 0.10.0 d'Ethereal :  
<http://www.ethereal.com/download.html>  
ou appliquer le correctif de l'éditeur :

- Avis de sécurité Debian DSA-407-1 :  
<http://www.debian.org/security/2004/dsa-407>
- Avis de sécurité RedHat RHSA-2004:001-01 :  
<http://rhn.redhat.com/errata/RHSA-2004-001.html>
- Avis de sécurité Mandrake MDKSA-2004:002 :  
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:002>

## 7 Documentation

- Bulletin de sécurité Ethereal enpa-sa-00012 :  
<http://www.ethereal.com/appnotes/enpa-sa-00012.html>
- Référence CVE CAN-2003-1012 :  
<http://cve.mitre.org/cgi-bin/cvname.cgi?name=CAN-2003-1012>
- Référence CVE CAN-2003-1013 :  
<http://cve.mitre.org/cgi-bin/cvname.cgi?name=CAN-2003-1013>

## Gestion détaillée du document

**08 janvier 2004** version initiale.

**14 janvier 2004** Ajout du bulletin de sécurité Mandrake.