



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 15 juillet 2003  
N° CERTA-2003-AVI-100-002

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-2003-AVI-100>

---

### Gestion du document

Référence	CERTA-2003-AVI-100-002
Titre	Multiples vulnérabilités d'Ethereal
Date de la première version	24 juin 2003
Date de la dernière version	15 juillet 2003
Source(s)	Bulletin de sécurité MDKSA-2003:070 de Mandrake Bulletin de sécurité DSA-324 de Debian Bulletin de sécurité enpa-sa-00010 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

Tous les systèmes avec `Ethereal` version 0.9.12 et antérieures.

## 3 Description

`Ethereal` est un renifleur réseau. Il permet l'analyse de données depuis le réseau ou à partir d'un fichier. De multiples vulnérabilités de type débordement de mémoire sont présentes dans `Ethereal`.

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 cette vulnérabilité afin d'exécuter du code arbitraire ou réaliser un déni de service sur la plate-forme utilisant une version vulnérable d'`Ethereal`.

## 4 Solution

Installer la version 0.9.13 d'Ethereal :

<http://www.ethereal.com>

ou appliquer le correctif de l'éditeur :

- Bulletin de sécurité DSA-324 de Debian :  
<http://www.debian.org/security/2003/dsa-324>
- Bulletin de sécurité MDKSA-2003:070 de Mandrake :  
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:070>
- Bulletin de sécurité RHSA-2003:203 de Red Hat :  
<http://rhn.redhat.com/errata/RHSA-2003-203.html>
- Bulletin de sécurité RHSA-2003:077-13 de Red Hat :  
<http://rhn.redhat.com/errata/RHSA-2003-077.html>

## 5 Documentation

- Bulletin de sécurité enpa-sa-00010 d'Ethereal :  
<http://www.ethereal.com/appnotes/enpa-sa-00010.html>
- Référence CVE CAN-2003-0428 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0428>
- Référence CVE CAN-2003-0429 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0429>
- Référence CVE CAN-2003-0431 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0431>
- Référence CVE CAN-2003-0432 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0432>

## Gestion détaillée du document

**24 juin 2003** version initiale.

**4 juillet 2003** ajout référence au bulletin RHSA-2003:203 de Red Hat.

**15 juillet 2003** ajout référence au bulletin RHSA-2003:077-13 de Red Hat.