

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité 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-2002-AVI-189>

---

### Gestion du document

Référence	CERTA-2002-AVI-189-001
Titre	Vulnérabilité dans Ethereal
Date de la première version	23 août 2002
Date de la dernière version	09 septembre 2002
Source(s)	Avis de sécurité Ethereal - Docid enpa-sa-00006
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

Tous les systèmes avec Ethereal version 0.9.5 et versions antérieures.

## 3 Résumé

Une vulnérabilité présente dans l'utilitaire réseau Ethereal permet à un utilisateur mal intentionné d'exécuter du code arbitraire et d'entraîner un déni de service sur la machine cible.

## 4 Description

Ethereal est un renifleur réseau. Il permet l'analyse de données directement depuis le réseau ou depuis un fichier.

Un débordement de mémoire dans la gestion du protocole de routage ISIS permet à un utilisateur mal intentionné, composant judicieusement un fichier destiné à être lu par `Ethereal` ou injectant un paquet malicieusement construit sur le réseau, d'exécuter du code arbitraire et d'entraîner un déni de service de l'application sur la machine cible.

## 5 Contournement provisoire

Désélectionner le protocole ISIS de la liste des protocoles supportés par `Ethereal`.

## 6 Solution

Télécharger la nouvelle version de `Ethereal` 0.9.6 (Consultez la section documentation).

## 7 Documentation

- Avis de sécurité de `Ethereal` - Docid ensa-sa-00006  
<http://www.ethereal.com/appnotes/enpa-sa-00006.html>
- Téléchargement de `Ethereal`  
<http://www.ethereal.com/download.html>
- Bulletin de sécurité DSA-162 de Debian :  
<http://www.debian.org/security/2002/dsa-162>
- Bulletin de sécurité RHSA-2002:169 de RedHat :  
<http://rhn.redhat.com/errata/RHSA-2002-169.html>

## Gestion détaillée du document

**23 août 2002** version initiale.

**09 septembre 2002** Ajouts des bulletins de sécurité de Debian et RedHat.