



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 décembre 2003
N° CERTA-2003-AVI-182-002

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-182>

Gestion du document

Référence	CERTA-2003-AVI-182-002
Titre	Multiples vulnérabilités d'Ethereal
Date de la première version	12 novembre 2003
Date de la dernière version	15 décembre 2003
Source(s)	Bulletin de sécurité enpa-sa-00011.html d'Ethereal Bulletin de sécurité RHSA-2003:323 de Red Hat
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` versions 0.9.15 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 une de ces vulnérabilités afin d'exécuter du code arbitraire ou réaliser un déni de service sur la plate-forme utilisant une version vulnérable d'`Ethereal`.

4 Contournement provisoire

Dans l'attente de l'application du correctif, désactiver les protocoles suivants : GTP, ISAKMP, MEGACO, SOCKS.

5 Solution

Installer la version 0.9.16 d'Ethereal :
<http://www.ethereal.com/download.html>

ou appliquer le correctif de l'éditeur :

- Bulletin de sécurité RHSA-2003:323 de Red Hat :
<http://rhn.redhat.com/errata/RHSA-2003-323.html>
- Bulletin de sécurité 200311-04 de Gentoo :
<http://www.securityfocus.com/advisories/6091>
- Bulletin de sécurité MDKSA-2003:114 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:114>

6 Documentation

- Bulletin de sécurité enpa-sa-00011 d'Ethereal :
<http://www.ethereal.com/appnotes/enpa-sa-00011.html>
- Référence CVE CAN-2003-0925 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0925>
- Référence CVE CAN-2003-0926 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0926>
- Référence CVE CAN-2003-0927 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0927>

Gestion détaillée du document

12 novembre 2003 version initiale.

25 novembre 2003 ajout référence au bulletin de sécurité de Gentoo.

15 décembre 2003 ajout référence au bulletin de sécurité de Mandrake.