Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 juillet 2004
N° CERTA-2004-AVI-166-004

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Ethereal

Gestion du document

Référence	CERTA-2004-AVI-166-004
Titre	Multiples vulnérabilités dans Ethereal
Date de la première version	14 mai 2004
Date de la dernière version	12 juillet 2004
Source(s)	Bulletin de sécurité enpsa-sa-00014 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

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

2 Systèmes affectés

Toutes les versions de Ethereal comprises entre les versions (incluses) 0.9.8 et 0.10.3.

3 Résumé

Quatre vulnérabilités dans Ethereal permettent à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter à distance 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 de ces vulnérabilités afin de réaliser un déni de service ou exécuter à distance du code arbitraire 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 : SIP, AIM, SPNEGO et MMSE.

6 Solution

Installer la version 0.10.4 d'Ethereal :
http://www.ethereal.com/download.html

7 Documentation

- Site Internet d'Ethereal :
  http://www.ethereal.com
- Bulletin de sécurité Ethereal enpa-sa-00014 du 13 mai 2004 :
  http://www.ethereal.com/appnotes/enpa-sa-00014.html
- Bulletin de sécurité Gentoo GLSA 200406-01 du 04 juin 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200406-01.xml
- Bulletin de sécurité RedHat RHSA-2004:234 du 09 juin 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-234.html
- Bulletin de sécurité FreeBSD pour Ethereal du 11 juillet 2004 :
  http://www.vuxml.org/freebsd/
- Mise à jour de sécurité du paquetage NetBSD ethereal :
  ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/net/ethereal/README.html
- Référence CVE CAN-2004-0504 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0504
- Référence CVE CAN-2004-0505 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0505
- Référence CVE CAN-2004-0506 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0506
- Référence CVE CAN-2004-0507 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0507

Gestion détaillée du document

14 mai 2004 version initiale.
04 juin 2004 ajout des références CVE.
07 juin 2004 ajout des références aux bulletins de sécurité Gentoo et NetBSD.
10 juin 2004 ajout de la référence au bulletin de sécurité Red Hat.
12 juillet 2004 ajout du site Internet d'Ethereal et de la référence au bulletin de sécurité FreeBSD.