Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 avril 2003
N° CERTA-2003-AVI-064-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Ethereal

Gestion du document

Référence	CERTA-2003-AVI-064-002
Titre	Vulnérabilité dans Ethereal
Date de la première version	26 mars 2003
Date de la dernière version	28 avril 2003
Source(s)	Bulletin de sécurité #60 de Georgi Guninski
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 à distance ;
- déni de service.

2 Systèmes affectés

Tous les systèmes avec `Ethereal` version 0.9.9 et versions antérieures.

3 Résumé

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

4 Description

`Ethereal` est un renifleur réseau. Il permet l'analyse de données depuis le réseau ou à partir d'un fichier.

Une vulnérabilité de type chaîne de format est présente dans la gestion du protocole `SOCKS`.

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`.

5 Contournement provisoire

Retirer le protocole `SOCKS` de la liste des protocoles supportés par `Ethereal`.

6 Solution

Installer la version 0.9.10 d'`Ethereal` :
http://www.ethereal.com
ou appliquer le correctif de l'éditeur :

- Bulletin de sécurité DSA-258 de Debian :
  http://www.debian.org/security/2003/dsa-258
- Bulletin de sécurité SuSE-SA:2003:019 de SuSE :
  http://www.suse.com/de/security/2003_019_ethereal.html
- Bulletin de sécurité 200303-10 de Gentoo :
  http://www.securityfocus.com/advisories/5076
- Bulletin de sécurité RHSA-2003:076-01 de RedHat :
  https://rhn.redhat.com/errata/RHSA-2003-076.html
- Bulletin de sécurité MDKSA-2003:051 de Mandrake :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:051

7 Documentation

- Bulletin de sécurité #60 "Ethereal format string bug, yet still ethereal much better than windows" de Georgi Guninski :
  http://www.guninski.com/etherre.html
- Bulletin de sécurité enpa-sa-00008 "SOCKS string format vulnerability in Ethereal 0.9.9" d'Ethereal :
  http://www.ethereal.com/appnotes/enpa-sa-00008.html
- Référence CVE CAN-2003-0081 et CAN-2003-0159 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0081
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0159

Gestion détaillée du document

26 mars 2003 version initiale.
24 avril 2003 ajout du bulletin de sécurité RedHat et d'une nouvelle référence CVE.
28 avril 2003 ajout du bulletin de sécurité Mandrake.