Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 avril 2005
N° CERTA-2005-AVI-103-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Ethereal

Gestion du document

Référence	CERTA-2005-AVI-103-002
Titre	Vulnérabilités dans Ethereal
Date de la première version	11 mars 2005
Date de la dernière version	29 avril 2005
Source(s)	Bulletin de sécurité LSS LSS-2005-03-04
Pièce(s) jointe(s)	

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

Ethereal 0.x.

3 Résumé

Plusieurs vulnérabilités présentes dans Ethereal permettent à un utilisateur mal intentionné d'exécuter du code arbitraire ou d'effectuer un déni de service à distance.

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 dépassement de la mémoire présente dans la fonction `dissect_a11_radius` permet à un utilisateur malveillant d'effectuer un déni de service ou d'exécuter du code arbitraire sur le système vulnérable au moyen de paquets `CDMA2000 A11` malicieusement construits.

Plusieurs vulnérabilités dans les routines de dissection des flux IAPP, Etheric, GPRS-LLC, JXTA, et sFlow permettent de réaliser un déni de service à distance.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site de l'éditeur :
  http://www.ethereal.com
- Bulletin de sécurité d'Ethereal enpa-sa-00018 du 11 mars 2005 :
  http://www.ethereal.com/appnotes/enpa-sa-00018.html
- Bulletin de sécurité LSS LSS-2005-03-04 du 08 mars 2005 :
  http://security.lss.hr/en/index.php?page=details&ID=LSS-2005-03-04
- Bulletin de sécurité de Gentoo GLSA 200503-16 du 13 mars 2005 :
  http://www.gentoo.org/security/en/glsa/glsa-200503-16.xml
- Bulletin de sécurité de Mandrake MDKSA-2005:053 du 15 mars 2005 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:053
- Bulletin de sécurité RedHat RHSA-2005:306-10 du 18 mars 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-306.html
- Bulletin de sécurité Debian DSA-718 du 28 avril 2005 :
  http://www.debian.org/security/2005/dsa-718
- Mise à jour du paquetage NetBSD Ethereal :
  ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/net/ethereal/README.html
- Référence CVE CAN-2005-0699 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0699
- Référence CVE CAN-2005-0704 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0704
- Référence CVE CAN-2005-0705 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0705
- Référence CVE CAN-2005-0739 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0739
- Référence CVE CAN-2005-0765 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0765
- Référence CVE CAN-2005-0766 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0766

Gestion détaillée du document

11 mars 2005 version initiale ;

21 mars 2005 ajout de plusieurs vulnérabilités. Ajout des références CVE, et des bulletins de sécurité d'Ethereal, de Gentoo, de Mandrake, de RedHat et de NetBSD ;

29 avril 2005 ajout du bulletin de sécurité Debian.