

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités 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-2004-AVI-228>

Gestion du document

Référence	CERTA-2004-AVI-228-004
Titre	Vulnérabilités dans Ethereal
Date de la première version	07 juillet 2004
Date de la dernière version	06 août 2004
Source(s)	Bulletin de sécurité Ethereal enpa-sa-00015 du 06 juillet 2004
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 d'Ethereal comprises entre les versions 0.8.15 et 0.10.4 (incluses).

3 Résumé

Trois vulnérabilités dans Ethereal permettent à un utilisateur mal intentionné de créer un déni de service ou d'exécuter 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 : iSNS, SMB et SNMP.

6 Solution

Installer la version 0.10.5 d'Ethereal.

Ethereal est téléchargeable à l'adresse suivante :

<http://www.ethereal.com/download.html>

7 Documentation

- Site Internet d'Ethereal :
<http://www.ethereal.com>
- Bulletin de sécurité Ethereal enpa-sa-00015 du 06 juillet 2004 :
<http://www.ethereal.com/appnotes/enpa-sa-00015.html>
- Bulletin de sécurité Gentoo GLSA 200407-08 du 09 juillet 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200407-08.xml>
- Bulletin de sécurité Mandrake MDKSA-2004:067 du 09 juillet 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:067>
- Bulletin de sécurité Debian DSA-528 du 17 juillet 2004 :
<http://www.debian.org/security/2004/dsa-528>
- Bulletin de sécurité RedHat RHSA-2004:378 du 05 août 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-378.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-2004-0633 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0633>
- Référence CVE CAN-2004-0634 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0634>
- Référence CVE CAN-2004-0635 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0635>

Gestion détaillée du document

07 juillet 2004 version initiale.

08 juillet 2004 ajout de la référence au bulletin de sécurité NetBSD.

12 juillet 2004 ajout des références aux bulletins de sécurité Gentoo, Mandrake et FreeBSD et ajout des références CVE.

19 juillet 2004 ajout de la référence au bulletin de sécurité Debian.

06 août 2004 ajout de la référence au bulletin de sécurité RedHat.