

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples 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-400>

Gestion du document

Référence	CERTA-2004-AVI-400-005
Titre	Multiples vulnérabilités dans Ethereal
Date de la première version	15 décembre 2004
Date de la dernière version	17 février 2005
Source(s)	Bulletin de sécurité ENPA-SA-00016 de 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

Ethereal versions 0.9.0 à 0.10.7 incluse.

3 Description

Ethereal est un renifleur réseau. Il permet l'analyse de données depuis le réseau ou à partir d'un fichier. Quatre vulnérabilités ont été découvertes dans Ethereal :

- une première vulnérabilité lors de l'analyse de certains paquets DICOM permet à un utilisateur mal intentionné de créer un déni de service. Cette vulnérabilité affecte les versions 0.10.4 à 0.10.7 d'Ethereal ;
- une vulnérabilité est due à une mauvaise manipulation du champ `timestamp` contenu dans l'entête des paquets RTP (Real-Time Transfert Protocol). L'exploitation de cette vulnérabilité par un individu mal intentionné permet d'arrêter le programme ou de créer un fichier temporaire pouvant occuper l'ensemble de l'espace disque disponible. Cette vulnérabilité affecte les versions 0.10.1 à 0.10.7 incluse ;

- une vulnérabilité présente dans la manipulation de paquets HTTP, peut sous certaines conditions, causer l'arrêter du programme. Cette vulnérabilité affecte les versions 0.10.1 à 0.10.7 d'Ethereal ;
- une vulnérabilité dans la gestion de certains paquets SMB (Server Message Block) permet à un utilisateur mal intentionné de créer un déni de service par l'envoi de paquets SMB malicieusement construits afin de consommer toutes les ressources CPU. Cette vulnérabilité affecte les versions 0.9.0 à 0.10.7 d'Ethereal.

4 Solution

Mettre à jour Ethereal avec la version 0.10.8 corrigeant ces vulnérabilités (cf. Documentation).

5 Documentation

- Bulletin de sécurité ENPA-SA-00016 de Ethereal :
<http://www.ethereal.com/appnotes/enpa-sa-00016.html>
- Bulletin de sécurité Gentoo GLSA-200412-15 du 19 décembre 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200412-15.xml>
- Bulletin de sécurité Mandrake MDKSA-2004:152 du 20 décembre 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:152>
- Bulletin de sécurité Debian DSA-613 du 21 décembre 2004 :
<http://www.debian.org/security/2004/dsa-613>
- Bulletin de sécurité RedHat RHSA-2005-037 du 15 février 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-037.html>
- Bulletin de sécurité FreeBSD "ethereal – multiple vulnerabilities" du 23 décembre 2004 :
<http://www.vuxml.org/freebsd/>
- Référence CVE CAN-2004-1139 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1139>
- Référence CVE CAN-2004-1140 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1140>
- Référence CVE CAN-2004-1141 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1141>
- Référence CVE CAN-2004-1142 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1142>

Gestion détaillée du document

15 décembre 2004 version initiale.

20 décembre 2004 Ajout référence au bulletin de sécurité de Gentoo. Ajout références CVE.

21 décembre 2004 Ajout référence au bulletin de sécurité de Mandrake.

22 décembre 2004 Ajout référence au bulletin de sécurité de Debian.

23 décembre 2004 Ajout référence au bulletin de sécurité de FreeBSD.

17 février 2005 Ajout référence au bulletin de sécurité RedHat.