

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de 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-2005-AVI-487>

Gestion du document

Référence	CERTA-2005-AVI-487-005
Titre	Vulnérabilité de Ethereal
Date de la première version	13 décembre 2005
Date de la dernière version	27 février 2006
Source(s)	Bulletin de sécurité Debian DSA-920 du 13 décembre 2005
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

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

2 Systèmes affectés

Ethereal versions 0.10.13 et antérieures.

3 Résumé

Une vulnérabilité dans Ethereal permet à un utilisateur mal intentionné de réaliser des dénis de service ou d'exécuter du code arbitraire à distance sur la plate-forme vulnérable.

4 Description

Le logiciel Ethereal permet de capturer des trames réseau et d'effectuer de multiples actions sur celles-ci afin de faciliter leur analyse.

Une vulnérabilité de type débordement de mémoire dans la fonction `dissect_ospf_v3_address_prefix()`,

fonction impliquée dans le traitement du protocole OSPF, permet à un utilisateur mal intentionné de réaliser des dénis de service ou d'exécuter du code arbitraire à distance sur la plate-forme vulnérable.

5 Contournement provisoire

Il est possible de désactiver l'interprétation OSPF par Ethereal :

- Sur plate-forme UNIX : `echo ospf » /.ethereal/disabled_protos;`
- sur plate-forme Windows : ajouter `ospf` au fichier `disabled_protos` qui se trouve dans le répertoire des préférences de l'utilisateur (typiquement `%APPDATA%\Ethereal\`).

6 Solution

Mettre à jour Ethereal à partir du code source en utilisant le dernier code source disponible via subversion (vérifier que le fichier `packet-ospf.c` est en révision 16507 ou toute révision supérieure).

Dans tous les cas, se référer au bulletin de l'éditeur pour l'obtention de correctifs (cf. Documentation).

7 Documentation

- Site Internet de Ethereal :
<http://www.ethereal.com>
- Bulletin de sécurité Ethereal enpa-sa-00022 du 27 décembre 2005 :
<http://www.ethereal.com/appnotes/enpa-sa-0002.html>
- La version 0.10.14 d'Ethereal est disponible à l'adresse suivante :
<http://www.ethereal.com/download.html>
- Bulletin de sécurité iDEFENSE #349 du 09 décembre 2005 :
<http://www.odefense.com/application/poi/display?id=349&type=vulnerabilities>
- Bulletin de sécurité Debian DSA-920 du 13 décembre 2005 :
<http://www.debian.org/security/2005/dsa-920>
- Bulletin de sécurité Mandriva MDKSA-2005:227 du 14 décembre 2005 :
<http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:227>
- Bulletin de sécurité Mandriva MDKSA-2006:002 du 03 janvier 2006 :
<http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:002>
- Bulletin de sécurité Gentoo GLSA 200512-06 du 14 décembre 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200512-06.xml>
- Bulletin de sécurité RedHat RHSA-2006:0156 du 11 janvier 2006 :
<https://rhn.redhat.com/errata/RHSA-2006-0156.html>
- Bulletin de sécurité SUSE SUSE-SR:2006:004 du 24 février 2006 :
http://www.novell.com/linux/security/advisories/2006_04_sr.html
- Référence CVE CAN-2005-3651 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3651>

Gestion détaillée du document

13 décembre 2005 version initiale.

15 décembre 2005 ajout des références aux bulletins de sécurité Mandriva et Gentoo.

29 décembre 2005 ajout de la référence au bulletin de sécurité Ethereal.

04 janvier 2006 ajout de la référence au bulletin de sécurité Mandriva.

13 janvier 2006 ajout de la référence au bulletin de sécurité RedHat.

27 février 2006 ajout de la référence au bulletin de sécurité SUSE.