

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Wireshark

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-2007-AVI-278>

Gestion du document

Référence	CERTA-2007-AVI-278-001
Titre	Vulnérabilités dans Wireshark
Date de la première version	27 juin 2007
Date de la dernière version	22 août 2007
Source(s)	Bulletin de sécurité Wireshark wnpa-sec-2007-002 du 25 juin 2007
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 à distance.

2 Systèmes affectés

– Wireshark, pour les versions antérieures à 0.99.6.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans Wireshark (Ethereal). Elles permettraient à une personne distante de provoquer une perturbation du service sur le système utilisant une version vulnérable.

4 Description

Plusieurs vulnérabilités ont été identifiées dans l'outil de capture et d'analyse de trafic réseau Wireshark. Ce dernier est la suite du projet Ethereal achevé en 2006.

Les vulnérabilités sont dues à de mauvaises manipulations de certaines trames, dont :

– une réponse HTTP particulière utilisant un mauvais encodage ;

- un paquet particulier DCP ETSI (ETSI *Distribution and Communication Protocol*);
- un paquet malformé SSL;
- un paquet malformé MMS;
- un paquet DHCP utilisé avec DOCSIS.

Certains fichiers de capture iSeries peuvent également provoquer une erreur à l'ouverture.

5 Solution

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

6 Documentation

- Notes des modifications apportées à la version 0.99.6 de Wireshark :
<http://www.wireshark.org/docs/relnotes/wireshark-0.99.6.html>
- Bulletin de sécurité Wireshark du 25 juin 2007 :
<http://www.wireshark.org/security/wnpa-2007-02.html>
- Bulletin de sécurité Gentoo GLSA-200708-12 du 16 août 2007 :
<http://www.gentoo.org/security/en/glsa/glsa-200708-12.xml>
- Bulletin de sécurité SuSE SUSE-SR:2007:015 du 03 août 2007 :
<http://lists.opensuse.org/opensuse-security-announce/2007-08/msg00003.html>
- Bulletin de sécurité Mandriva MDKSA-2007:145 du 10 juillet 2007 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:145>
- Bulletin de sécurité Debian DSA-1322 du 27 juin 2007 :
<http://www.debian.org/security/2007/dsa-1322>
- Référence CVE CVE-2007-3389 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3389>
- Référence CVE CVE-2007-3390 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3390>
- Référence CVE CVE-2007-3391 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3391>
- Référence CVE CVE-2007-3392 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3392>
- Référence CVE CVE-2007-3393 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3393>

Gestion détaillée du document

27 juin 2007 version initiale.

22 août 2007 ajout des références aux bulletins de sécurité Gentoo, Mandriva, SuSE et Debian.