

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples 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-2011-AVI-503>

Gestion du document

Référence	CERTA-2011-AVI-503-001
Titre	Multiples vulnérabilités dans Wireshark
Date de la première version	12 septembre 2011
Date de la dernière version	20 septembre 2011
Source	Bulletins de sécurité Wireshark du 07 septembre 2011
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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

- Wireshark versions 1.6.0 à 1.6.1 ;
- Wireshark versions 1.4.0 à 1.4.8.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans le logiciel Wireshark. Elles permettent à une personne malintentionnée de provoquer une perturbation du service ou d'exécuter des commandes arbitraires à distance sur le système utilisant une version vulnérable.

4 Description

Plusieurs vulnérabilités ont été identifiées dans le logiciel Wireshark :

- des bogues dans l'interprétation des formats CSN.1 et IKE permettent à une personne malintentionnée distante de provoquer un déni de service au moyen de paquets spécialement conçus ;
- une vulnérabilité présente au chargement de fichiers de capture réseau permet de provoquer un déni de service au moyen d'un fichier spécialement conçu ;
- l'exécution de scripts LUA arbitraires est possible grâce à l'utilisation d'une méthode similaire au « DLL hijacking ».

5 Solution

Les versions 1.6.2 et 1.4.9 de Wireshark corrigent ces vulnérabilités.

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

6 Documentation

- Bulletins de sécurité Wireshark du 07 septembre 2011 :
<http://www.wireshark.org/security/wnpa-sec-2011-13.html>
<http://www.wireshark.org/security/wnpa-sec-2011-14.html>
<http://www.wireshark.org/security/wnpa-sec-2011-15.html>
<http://www.wireshark.org/security/wnpa-sec-2011-16.html>
- Référence CVE CVE-2011-3266 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3266>
- Référence CVE CVE-2011-3360 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3360>
- Référence CVE CVE-2011-3482 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3482>
- Référence CVE CVE-2011-3483 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3483>
- Référence CVE CVE-2011-3484 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3484>

Gestion détaillée du document

12 septembre 2011 version initiale.

20 septembre 2011 ajout de références CVE.