

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-125>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2011-AVI-125 |
| Titre | Multiples vulnérabilités dans Wireshark |
| Date de la première version | 03 mars 2011 |
| Date de la dernière version | – |
| Source(s) | Bulletins de sécurité wpna-sec-2011-03 et wpna-sec-2011-04 du 01 mars 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 1.2.0 à 1.2.14 (incluse) ;
- *Wireshark* versions 1.4.0 à 1.4.3 (incluse).

3 Résumé

De multiples vulnérabilités dans *Wireshark* permettent d'exécuter du code arbitraire ou de réaliser un déni de service à distance.

4 Description

De multiples vulnérabilités ont été découvertes dans *Wireshark* :

- une désallocation de pointeur non-initialisé peut survenir lors de la lecture d'un fichier au format pcap-ng (CVE-2011-0538) ;

- un paquet de très grande taille dans un fichier pcap-ng peut provoquer un arrêt inopiné de *Wireshark* ;
- un débordement de mémoire peut se produire lors du traitement d'un fichier au format Nokia DCT3 (CVE-2011-0713) ;
- *Wireshark* peut s'arrêter brutalement lors de la lecture de paquets 6LoWPAN sur des systèmes 32 bits ;
- des débordements de mémoire existent dans les préprocesseurs LDAP et SMB ;
- des filtres LDAP peuvent provoquer une consommation excessive de la mémoire.

L'exploitation de ces vulnérabilités permet la réalisation d'un déni de service ou l'exécution de code arbitraire à distance.

5 Solution

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

6 Documentation

- Bulletins de sécurité wpna-sec-2011-03 et wpna-sec-2011-04 du 01 mars 2011 :
<http://www.wireshark.org/security/wnpa-sec-2011-03.html>
<http://www.wireshark.org/security/wnpa-sec-2011-04.html>
- Référence CVE CVE-2011-0538 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0538>
- Référence CVE CVE-2011-0713 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0713>

Gestion détaillée du document

03 mars 2011 version initiale.