

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-2009-AVI-463>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2009-AVI-463 |
| Titre | Multiples vulnérabilités dans Wireshark |
| Date de la première version | 28 octobre 2009 |
| Date de la dernière version | – |
| Source(s) | Bulletins de sécurité Wireshark wnpa-sec-2009-07 et wnpa-sec-2009-08 du 26 octobre 2009 |
| 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 0.10.x ;
- Wireshark 1.0.x ;
- Wireshark 1.2.x.

3 Résumé

Plusieurs vulnérabilités présentes dans *Wireshark* permettent à un utilisateur distant malintentionné de provoquer un déni de service.

4 Description

Plusieurs vulnérabilités sont présentes dans Wireshark :

- La première (CVE-2009-2560), n'affectant pas les versions supérieures à 1.2.0, concerne l'analyseur de protocole RADIUS ;
- la seconde (CVE-2009-3549), n'affectant que la branche 1.2.x, est relative à l'analyseur de protocole Pa1talk ;
- la troisième (CVE-2009-3550) concerne l'analyseur de protocole DCERPC/NT ;
- la dernière (CVE-2009-3551), n'affectant que la branche 1.2.x, est relative à l'analyseur de protocole SMB.

Toutes ces vulnérabilités permettent à un utilisateur distant malintentionné de provoquer un déni de service de l'application vulnérable.

5 Solution

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

6 Documentation

- Bulletins de sécurité Wireshark wnpa-sec-2009-07 et wnpa-sec-2009-08 du 26 octobre 2009 :
<http://www.wireshark.org/security/wnpa-sec-2009-07.html>
<http://www.wireshark.org/security/wnpa-sec-2009-08.html>
- Référence CVE CVE-2009-2560 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2560>
- Référence CVE CVE-2009-3549 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3549>
- Référence CVE CVE-2009-3550 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3550>
- Référence CVE CVE-2009-3551 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3551>

Gestion détaillée du document

28 octobre 2009 version initiale.