

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-554>

Gestion du document

Référence	CERTA-2009-AVI-554-001
Titre	Multiples vulnérabilités dans Wireshark
Date de la première version	18 décembre 2009
Date de la dernière version	24 décembre 2009
Source(s)	Bulletin de sécurité Wireshark wnpa-sec-2009-09 du 17 décembre 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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

Les versions de Wireshark de la 0.9.0 à la 1.2.4 incluses.

3 Résumé

Plusieurs vulnérabilités dans *Wireshark* permettant de provoquer un déni de service à distance et de contourner la politique de sécurité ont été corrigées.

4 Description

Des vulnérabilités dans *Wireshark* concernant le traitement des protocoles réseau SNA, SMB, SMB2 et IPMI ont été corrigées. Une personne malveillante distante pourrait les exploiter au moyen de trames spécialement réalisées pour provoquer un déni de service ou contourner la politique de sécurité.

5 Solution

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

6 Documentation

- Bulletin de sécurité Wireshark wnpa-sec-2009-09 du 17 décembre 2009 :
<http://www.wireshark.org/security/wnpa-sec-2009-09.html>
- item Bulletin de sécurité Fedora FEDORA-2009-13592 du 23 décembre 2009 :
<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg01248.html>
- Référence CVE CVE-2009-4376 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4376>
- Référence CVE CVE-2009-4377 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4377>
- Référence CVE CVE-2009-4378 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4378>

Gestion détaillée du document

18 décembre 2009 version initiale.

24 décembre 2009 ajout des références CVE et de la référence au bulletin de sécurité Fedora.