Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 06 mars 2009
N° CERTA-2009-AVI-055-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Wireshark

Gestion du document

Référence	CERTA-2009-AVI-055-001
Titre	Vulnérabilités dans Wireshark
Date de la première version	10 février 2009
Date de la dernière version	06 mars 2009
Source(s)	Bulletin de sécurité Wireshark wnpa-sec-2009-01 du 06 février 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

- Wireshark (anciennement Ethereal), pour les versions 0.99.6 à 1.0.5 incluse.

3 Résumé

Des vulnérabilités ont été identifiées dans Wireshark. Elles permettent à une personne distante de perturber le service de capture et d'affichage de trames réseau et donc de contourner la politique de sécurité mise en place.

4 Description

Des vulnérabilités ont été identifiées dans Wireshark. L'application ne manipule pas correctement la variable d'environnement `HOME` (pour les systèmes qui ne sont pas sous Windows). Elle ne gère également pas de manière satisfaisante certains fichiers de capture Netscreen ou Tektronix K12 en texte.

Ces vulnérabilités peuvent être exploitées par une personne locale ou distante afin de perturber le service de capture et d'affichage de trames réseau.

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-2009-01 du 06 février 2009 :
  http://www.wireshark.org/security/wnpa-sec-2009-01.html
- Bulletin de sécurité Red Hat RHSA-2009:0313 du 04 mars 2009 :
  http://rhn.redhat.com/errata/RHSA-2009-0313.htm
- Bulletin de sécurité SuSE SuSE-SR:2009:005 du 02 mars 2009 :
  http://lists.opensuse.org/opensuse-security-announce/2009-03/msg00000.html
- Référence CVE CVE-2009-0599 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0599
- Référence CVE CVE-2009-0600 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0600

Gestion détaillée du document

10 février 2009 version initiale.
06 mars 2009 ajout des références CVE et des bulletins de sécurité Red Hat et SuSE.