Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 juillet 2010
N° CERTA-2010-AVI-260-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Wireshark

Gestion du document

Référence	CERTA-2010-AVI-260-002
Titre	Vulnérabilités dans Wireshark
Date de la première version	11 juin 2010
Date de la dernière version	02 juillet 2010
Sources	Bulletins de sécurité Wireshark wnpa-sec-2010-05 du 09 juin 2010 Bulletins de sécurité Wireshark wnpa-sec-2010-06 du 09 juin 2010
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 :
- branche 1.2 : versions 1.20 à 1.2.8 ;
- branches précédentes : version 1.0.13 et versions antérieures.

3 Résumé

Plusieurs vulnérabilités présentes dans Wireshark permettent à un utilisateur malveillant de réaliser un déni de service à distance, voire d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités de Wireshark ont été publiées et corrigées :

- l'analyseur SMB peut déréférencer un pointeur nul ;
- l'analyseur SMB PIPE peut déréférencer un pointeur nul ;
- l'analyseur ASN.1 BER peut provoquer un débordement de pile ;
- la *SigComp Universal Decompressor Virtual Machine* peut partir dans une boucle infinie ;
- la *SigComp Universal Decompressor Virtual Machine* peut provoquer un débordement de tampon.

5 Solution

Les versions 1.0.14 et 1.2.9 remédient à ces problèmes.
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-2010-05 et wnpa-sec-2010-06 du 09 juin 2010 :
  http://www.wireshark.org/security/wnpa-sec-2010-05.html
  http://www.wireshark.org/security/wnpa-sec-2010-06.html
- Bulletin de sécurité Debian DSA 2066 du 01 juillet 2010 :
  http://www.debian.org/security/2010/dsa-2066
- Bulletin de sécurité Mandriva MDVSA-2010:113 du 10 juin 2010 :
  http://www.mandriva.com/security/advisories?name=MDVSA-2010:113
- Référence CVE CVE-2010-2283 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2283
- Référence CVE CVE-2010-2284 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2284
- Référence CVE CVE-2010-2285 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2285
- Référence CVE CVE-2010-2286 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2286
- Référence CVE CVE-2010-2287 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2287

Gestion détaillée du document

11 juin 2010 version initiale.
16 juin 2010 ajout des références CVE.
02 juillet 2010 ajout des références aux bulletins de sécurité Mandriva et Debian.