



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 août 2010
N° CERTA-2010-AVI-348-001

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-2010-AVI-348>

Gestion du document

Référence	CERTA-2010-AVI-348-001
Titre	Multiples vulnérabilités dans Wireshark
Date de la première version	30 juillet 2010
Date de la dernière version	17 août 2010
Source(s)	Les bulletins de sécurité Wireshark wnpa-sec-2010-07 et wnpa-sec-2010-08 du 29 juillet 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

Les versions de Wireshark 0.10.8 à 1.0.14 et 1.2.0 à 1.2.9.

3 Résumé

Plusieurs vulnérabilités relatives au traitement de différents protocoles et permettant, entre autre, l'exécution de code arbitraire à distance ont été corrigées dans Wireshark.

4 Description

Des vulnérabilités dans le traitement de certains protocoles, dont ASN.1 BER, GSM A RR et IPMI ont été corrigées dans Wireshark. Elles peuvent être utilisées par une personne malintentionnée distante pour exécuter du code arbitraire ou provoquer un déni de service au moyen de trames réseaux spécialement réalisées.

5 Solution

LA version 1.2.10 remédie à ces vulnérabilités.

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-2010-07` et `wnpa-sec-2010-08` du 29 juillet 2010 :
<http://www.wireshark.org/security/wnpa-sec-2010-07.html>
<http://www.wireshark.org/security/wnpa-sec-2010-08.html>
- Référence CVE CVE-2010-2992 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2992>
- Référence CVE CVE-2010-2993 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2993>
- Référence CVE CVE-2010-2994 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2994>
- Référence CVE CVE-2010-2995 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2995>

Gestion détaillée du document

30 juillet 2010 version initiale.

17 août 2010 rectification des références CVE.