

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de Snort

---

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-2007-AVI-095>

---

### Gestion du document

Référence	CERTA-2007-AVI-095-001
Titre	Vulnérabilité de Snort
Date de la première version	20 février 2007
Date de la dernière version	13 mars 2007
Source(s)	Alerte TA07-050A de l'US-CERT
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.

## 2 Systèmes affectés

- *Snort* versions 2.6.1, 2.6.1.1, 2.6.1.2, 2.7.0 beta 1 ;
- *Sourcefire Intrusion Sensor* versions 4.1.x, 4.5.x, 4.6.x avec SEU antérieur à SEU 64 ;
- *Sourcefire Intrusion Sensor for Crossbeam* versions 4.1.x, 4.5.x, 4.6.x avec SEU antérieur à SEU 64.

## 3 Résumé

Une erreur de traitement par le préprocesseur DCE/RPC de *Snort* permettrait à un utilisateur malveillant d'exécuter du code arbitraire à distance.

## 4 Description

*Sourcefire Snort* est un logiciel libre de système de détection d'intrusion. Une erreur de traitement par le préprocesseur DCE/RPC de *Snort* conduit à un mauvais réassemblage de trafic fragmenté DCE/RPC et SMB. Cette erreur permettrait à un utilisateur malveillant d'exécuter du code arbitraire à distance.

## 5 Solution

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

## 6 Documentation

- Alerte de sécurité de l'US-CERT TA07-050A du 19 février 2007 :  
<http://www.us-cert.gov/cas/techalerts/TA07-050A.html>
- Bulletin de la version 2.6.1.3 de Sourcefire :  
[http://www.snort.org/docs/release\\_notes/release\\_notes\\_2613.txt](http://www.snort.org/docs/release_notes/release_notes_2613.txt)
- Référence CVE CVE-2006-5276 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5276>
- Mise à jour pour Gentoo :  
<http://www.gentoo.org/security/en/gisa/gisa-200703-01.xml>

## Gestion détaillée du document

**20 février 2007** version initiale;

**13 mars 2007** ajout de la référence au correctif pour Gentoo.