Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 janvier 2013
N° CERTA-2013-AVI-056

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Snort

Gestion du document

Référence	CERTA-2013-AVI-056
Titre	Vulnérabilité dans Snort
Date de la première version	22 janvier 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité Snort du 17 janvier 2013
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 version 2.9.4.0
- Snort version 2.9.3.1
- Snort version 2.9.2.3

Les autres versions sont potentiellement affectées

3 Résumé

Une vulnérabilité a été corrigée dans *Snort*. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance au moyen de réponses DCE/RPC spécialement conçues.

4 Solution

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

5 Documentation

- Bulletin de sécurité Snort du 17 janvier 2013 :
  http://blog.snort.org/2013/01/sourcefire-vrt-certified-snort-rules_18.html
  http://www.snort.org/vrt/docs/ruleset_changelogs/changes-2013-01-17.html

Gestion détaillée du document

22 janvier 2013 version initiale.