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 mai 2008
N° CERTA-2008-AVI-261

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité d'un préprocesseur de Snort

Gestion du document

Référence	CERTA-2008-AVI-261
Titre	Vulnérabilité d'un préprocesseur de Snort
Date de la première version	22 mai 2008
Date de la dernière version	–
Source(s)	Avis de sécurité iDefense 701 du 21 mai 2008
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

Contournement de la politique de sécurité.

2 Systèmes affectés

Les versions de Snort antérieures à 2.8.1 et disposant d'un « préprocesseur » activé `frag3`.

3 Résumé

Une vulnérabilité a été identifiée dans Snort. Elle permettrait de contourner la politique de détection mise en place.

4 Description

Une vulnérabilité a été identifiée dans le préprocesseur `frag3` de Snort. Celui-ci réassemble des trames IP ayant été fragmentées. Il considère par ailleurs que tous les fragments doivent avoir une valeur `Time-To-Live` relativement proche du fragment initial. Dans le cas contraire, le paquet ne sera pas inspecté avec les règles de détection mises en place.

Cette vulnérabilité peut être exploitée pour contourner la politique de détection.

5 Solution

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

6 Documentation

- Référence CVE CVE-2008-1804 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1804
- Bulletin de sécurité iDefense 701 du 21 mai 2008 :
  http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=701
- Notes de changement de Snort (sourcefire) :
  http://cvs.snort.org/viewcvs.cgi/snort/ChangeLog?rev=1.534.2.11

Gestion détaillée du document

22 mai 2008 version initiale.