Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 mars 2003
N° CERTA-2003-AVI-035

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le préprocesseur RPC de snort

Gestion du document

Référence	CERTA-2003-AVI-035
Titre	Vulnérabilité dans le préprocesseur RPC de snort
Date de la première version	04 mars 2003
Date de la dernière version	–
Source(s)	Site web snort.org Avis de sécurité ISS
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 avec les privilège du processus `snort`.

2 Systèmes affectés

Toutes les versions de `snort` de 1.8 à 1.9 incluse.
La version 1.9.1 corrige cette vulnérabilité.

3 Résumé

Il est possible d'effectuer un débordement de mémoire du préprocesseur `RPC` du logiciel `snort`.

4 Description

`snort` est un outil de détection d'intrusion. Dans la version 1.8 a été développée une fonction de détection des attaques par fragmentation sur les services `RPC`.

Un vulnérabilité de type débordement de mémoire présente dans cette partie du programme permet à un utilisateur mal intentionné d'exécuter du code arbitraire avec les privilèges du processus `snort` sur la machine hébergeant le logiciel de détection d'intrusion.

Il n'est pas nécessaire d'établir une connexion `RPC` avec une machine située dans le sous réseau surveillé par la sonde `snort` pour exploiter cette vulnérabilité. L'attaque peut se faire en émettant des paquets `RPC` habilement construit en direction de ce réseau même si la machine cible ne possède pas de service `RPC` en écoute.

5 Contournement provisoire

S'il n'est pas possible de mettre à jour le logiciel `snort` vulnérable, la détection d'intrusion par `RPC` peut-être désactivée dans le fichier `snort.conf` en remplaçant la ligne suivante :

```
preprocessor rpc_decode
```

par :

```
#preprocessor rpc_decode
```

6 Solution

Installer la version 1.9.1 de `snort`.

7 Documentation

- Site web de snort :
  http://www.snort.org
- Bulletin de sécurité ISS :
  http://www.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21951

Gestion détaillée du document

04 mars 2003 version initiale.