



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 octobre 2005
N° CERTA-2005-AVI-408

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-2005-AVI-408>

Gestion du document

Référence	CERTA-2005-AVI-408
Titre	Vulnérabilité de Snort
Date de la première version	19 octobre 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Snort du 18 octobre 2005
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

Versions de Snort antérieures à la version 2.4.3.

3 Description

Snort est un logiciel libre de détection d'intrusion.

Une vulnérabilité dans le pré-processeur Back Orifice de Snort permet à un utilisateur mal intentionné, au moyen d'un paquet habilement construit, d'exécuter du code arbitraire à distance sur la machine vulnérable.

4 Contournement provisoire

Désactiver le pré-processeur Back Orifice. Pour cela, commenter la ligne `preprocessor bo` dans le fichier de configuration Snort `snort.conf`.

Redémarrer Snort afin de prendre en compte les modifications.

5 Solution

Mettre à jour Snort en version 2.4.3.

Snort est téléchargeable à l'adresse suivante :

<http://www.snort.org/dl/>

6 Documentation

- Site Internet de Snort :
<http://www.snort.org>
- Bulletin de sécurité Snort du 18 octobre 2005 :
<http://www.snort.org/pub-bin/snortnews.cgi#99>
- Liste des changements dans Snort 2.4.3 :
http://www.snort.org/docs/change_logs/2.4.3/Changelog.txt
- Bulletin de sécurité US-CERT VU#175500 du 18 octobre 2005 :
<http://www.kb.cert.org/vuls/id/175500>
- Référence CVE CAN-2005-3252 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3252>

Gestion détaillée du document

19 octobre 2005 version initiale.