

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le préprocesseur stream4 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-2003-AVI-078>

Gestion du document

Référence	CERTA-2003-AVI-078
Titre	Vulnérabilité dans le préprocesseur stream4 de Snort
Date de la première version	18 avril 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité CORE-2003-0307 de Core Security Technologies Avis CA-2003-13 du CERT/CC
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

- Déni de service ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

Snort versions 1.8 à 2.0 beta.

3 Résumé

Une vulnérabilité présente dans le préprocesseur `stream4` de snort peut être exploitée afin d'exécuter du code arbitraire à distance sur la machine utilisant une version vulnérable de snort.

4 Description

Stream4 est un préprocesseur utilisé par Snort, un outil de détection d'intrusions. Stream4 permet de réassembler les segments TCP avant la recherche de signatures d'attaques.

Au moyen de paquets judicieusement composés, un utilisateur mal intentionné peut exploiter une vulnérabilité de type débordement de mémoire présente dans le préprocesseur stream4 afin d'exécuter du code arbitraire sur la machine utilisant une version vulnérable de snort.

5 Contournement provisoire

En attendant d'installer une version non vulnérable, désactiver le préprocesseur stream4 dans le fichier snort.conf.

6 Solution

La version 2.0.0 disponible sur le site de snort corrige cette vulnérabilité.

Site de snort :

<http://www.snort.org>

7 Documentation

- Référence CVE CAN-2003-0209 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0209>
- Bulletin de sécurité CORE-2003-0307 de Core Security Technologies :
<http://www.coresecurity.com/common/showdoc.php?idx=313&idxseccion=10>
- Avis CA-2003-13 du CERT/CC :
<http://www.cert.org/advisories/CA-2003-13.html>
- Avis de sécurité "Integer overflow in Stream4" de snort :
<http://www.snort.org/advisories/snort-2003-04-16-1.txt>

Gestion détaillée du document

18 avril 2003 version initiale.