Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 novembre 2001
N° CERTA-2001-AVI-138

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des SYNCOOKIES dans le noyau Linux

Gestion du document

Référence	CERTA-2001-AVI-138
Titre	Vulnérabilité des SYNCOOKIES dans le noyau Linux
Date de la première version	07 novembre 2001
Date de la dernière version	–
Source(s)	Avis de sécurité SuSE-SA:2001:039
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

Systèmes Linux utilisant l'option SYNCOOKIES et le filtrage de connexions "à état" basé sur le drapeau SYN.

3 Résumé

Une vulnérabilité dans l'implémentation du mécanisme SYNCOOKIES du noyau Linux permet à un utilisateur mal intentionné de réaliser des connexions non autorisées sur un système réalisant un filtrage de connexions "à état" basé sur le drapeau SYN.

4 Description

Un système peut utiliser le mécanisme SYNCOOKIES pour se protéger des attaques par déni de service de type TCP-SYN-FLOOD.

La commande `sysctl net.ipv4.tcp_syncookies` ou `cat /proc/sys/net/ipv4/tcp_syncookies` permet de voir si les SYNCOOKIES sont utilisés sur le système (0 signifie que le mécanisme est désactivé).

Une vulnérabilité dans l'implémentation du mécanisme SYNCOOKIES du noyau Linux permet à un utilisateur mal intentionné de réaliser des connexions non autorisées sur un système réalisant un filtrage de connexions "à état" basé sur le drapeau SYN (options -y pour `ipchains` ou –syn pour `iptables`).

L'exploitation de cette vulnérabilité n'est toutefois possible que si une attaque de type TCP-SYN-FLOOD est déclenchée sur un port non filtré, entraînant du même coup la mise en oeuvre des SYNCOOKIES pour les ports filtrés.

5 Contournement provisoire

Dans l'attente de la mise à jour du noyau Linux, désactiver le mécanisme SYNCOOKIES au moyen de la commande `sysctl -w net.ipv4.tcp_syncookies=0` ou `echo 0 > /proc/sys/net/ipv4/tcp_syncookies`.

6 Solution

Consultez l'éditeur pour obtenir une mise à jour correspondant à votre distribution.

7 Documentation

- "SYN cookies"
  http://cr.yp.to/syncookies.html ;
- Avis de sécurité SuSE: SuSE-SA:2001:039;
- Avis de sécurité RedHat: RHSA-2001:142-15.

Gestion détaillée du document

07 novembre 2001 version initiale.