Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 8 juin 2000
CERTA-2000-ALE-006

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Deni de service sous Firewall-1

Résumé

Une vulnérabilité dans la journalisation des attaques liées à la fragmentation a été découverte sur Firewall-1. Cette vulnérabilité peut avoir pour conséquence de saturer les ressources du système hébergeant le garde barrière. Il est à noter que d'autres gardes barrières peuvent être sujets à une vulnérabilité du même type.

Gestion du document

Date de la première version	8 juin 2000
Date de la dernière version	-
Sources	voir section 4

TAB. 1: gestion du document

1 Description

L'attaque consiste à envoyer des paquets fragmentés illégaux (par exemple des paquets ICMP du type "ping of death"), de façon à saturer la journalisation de ce type d'attaque. L'activité du CPU est alors entièrement dédiée à ce travail de trace.

Notons que la règle par défaut la plus restrictive (interdire tout) ne vous met pas à l'abri de ce type d'attaque. De plus Firewall-1 n'est pas en mesure de tracer ce type d'attaque.

2 Détection d'attaque

En consultant le fichier /var/log/messages sous Unix ou le NTEvent Viewer sous NT, on constate une grande quantité de messages du type :

```
packet size too big (65529) from 0x0g013c5f, ip_p=1
```

Ces messages et une utilisation hors norme du temps CPU sont le signe que vous êtes sous une attaque du type déni de service par fragmentation.

3 Solution

Une solution temporaire consiste à supprimer la journalisation des événements liés au noyau de Firewall-1. Cette action ne touche en principe pas à la journalisation des règles standards de filtrage. En revanche certains messages relatifs à la translation d'adresse risquent d'être perdus.

```
$FWDIR/bin/fw ctl debug -buf
```

Cette commande peut être ajoutée à la commande de démarage de Firewall-1 (FWDIR/bin/fw/fwstart) afin de la prendre en compte lorsque le garde barrière est relancé.

Il est également possible d'utiliser un système de détection d'intrusion qui bloquera la source émettant des paquets fragmentés illégaux (cette solution ne fonctionnant pas si l'adresse source est usurpée).

4 Références

– Check Point IP Fragment-diven DoS Alert :
http://www.checkpoint.com/techsupport/alerts/ipfrag_dos.html
– FW-1 IP Fragmentation Vulnerability :
http://www.entract.com/ lspitz/fwtable.html
– Site de securityfocus :
http://securityfocus.com/vdb/
– Avis du CERT IST.
– Institute for security Technology Studies :
http://www.phoneboy.com/fw1

Historique du document

8 juin 2000 première version