La faille de sécurité Linux Fragnesia

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 13 mai 2026

https://www.bortzmeyer.org/fragnesia.html

Ah, contrairement à CopyFail <https://www.bortzmeyer.org/copyfail.html> et DirtyFrag <https://www.bortzmeyer.org/dirtyfrag.html>, la faille de sécurité Linux Fragnesia <https://github.com/v12-security/pocs/tree/main/fragnesia> ne semble pas marcher sur mes machines.

Sur une Debian 13 (évidemment une machine sacrifiable), à jour donc ayant un noyau protégé contre DirtyFrag <https://www.bortzmeyer.org/dirtyfrag.html>, mais sans le contournement consistant à bloquer le chargement des modules via un `/etc/modprobe.d/dirtyfrag.conf` :

```
toto@s55827:~$  git clone https://github.com/v12-security/pocs.git
toto@s55827:~$ cd pocs/fragnesia/
[Lire le code source, renoncer car il est trop compliqué.]
toto@s55827:~/pocs/fragnesia$ gcc -o fragnesia fragnesia.c
toto@s55827:~/pocs/fragnesia$ ./fragnesia
[*] uid=1000 euid=1000 gid=1000 egid=1000
[*] mode=xfrm_espintcp_pagecache_replace collateral=after

[*] target=/usr/bin/su size=84360
outer_write_open_denied=1 errno=13 (Permission denied)
userns_setup: outer_uid=1000 outer_gid=1000 ns_uid=0 ns_gid=0
netns_setup=1
loopback_up=1
namespace_gate_failed: XFRM_MSG_NEWSA ack errno=22 (Invalid argument)
toto@s55827:~/pocs/fragnesia$ su
Password:
```

Les modules sont bien chargés :

```
toto@s55827:~/pocs/fragnesia$ lsmod | egrep esp\|xfr
esp6                   32768  0
esp4                   28672  0
xfrm_user              69632  0
xfrm_algo              16384  3 esp6,esp4,xfrm_user
```

Donc, le programme d'exploitation de la faille ne marche pas sur Debian. Reste à savoir si c'est juste une bogue du POC (peut-être spécifique à Debian), qu'on pourrait corriger, ou bien si Fragnesia n'est pas si universelle que ça. En attendant, j'ai quand même réactivé ce contournement sur toutes mes machines, à tout hasard (et parce qu'il n'a pas trop d'inconvénients si on ne fait pas d'IPsec) :

```
sh -c "printf 'install esp4 /bin/false\ninstall esp6 /bin/false\ninstall rxrpc /bin/false\n' > /etc/modprobe
```

D'autant plus que le POC de Fragnesia semble marcher sur Ubuntu, Fedora et Arch <https://blacksky.community/profile/did:plc:jtlcuolp6oiffznfic7i2rr5/post/3mlqnskhcps2x>.

decio <https://infosec.exchange/@decio> a testé sur Kali, même « problème ». Cela semble dû au fait que l'ESP dans TCP ne soit pas activé du tout :

```
root@s55827 ~ # grep ESPINTCP /boot/config-$(uname -r)
# CONFIG_INET_ESPINTCP is not set
# CONFIG_INET6_ESPINTCP is not set
```