main | Go to file | Code

0xdeadbeefnetwork Update README.md	1701eee · 18 hours ago	
ipv6	ipv6: add esp6 dual	20 hours ago
README.md	Update README.md	18 hours ago
aa-rootns.c	Copy Fail 2: Electric Bo...	yesterday
copyfail2.c	Copy Fail 2: Electric Bo...	yesterday
run.sh	Copy Fail 2: Electric Bo...	yesterday

README

Copy Fail 2: Electric Boogaloo

Unprivileged Linux LPE via xfrm ESP-in-UDP MSG_SPLICE_PAGES no-COW fast path. Page-cache write into any readable file. Overwrites a nologin line in `/etc/passwd` with `sick::0:0:...:/:/bin/bash` and `su s` into it. Same class as Copy Fail (CVE-2026-31431), different subsystem.

Bug: https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net.git/commit/?id=f4c50a4034e62ab75f1d5cdd191dd5f9c77fdff4

Build

```
sudo apt install -y libssl-dev gcc
gcc -O2 -Wall copyfail2.c -o copyfail2 -lcrypto
gcc -O2 -Wall aa-rootns.c -o aa-rootns
```

Run

```
./run.sh           # install + drop into root sh
./run.sh --clean   # revert /etc/passwd via the s
```

Adds passwordless uid-0 user `sick` to `/etc/passwd`, then `exec su - sick`. PAM `nullok` accepts the empty password silently — no input needed. The `sick` line stays in `/etc/passwd` — re-run drops straight back into root. State for `--clean` is stashed at `/var/tmp/.cf2.state`.

No sudo. esp4 / xfrm_user / xfrm_algo autoload via the userns netlink path.

Tested

distro	kernel	result
Ubuntu 22.04 LTS	5.15.0-176-generic	not vulnerable*
Ubuntu 24.04 LTS	6.8.0-110-generic	root
Debian 13	6.12.74	root
Arch	6.19.11-arch1-1	root
Fedora 43	6.19.14-200.fc43	root
Ubuntu 26.04 LTS	7.0.0-15-generic	root

IPv6

Same bug exists in `esp6_input` and is not covered by the v4 fix `f4c50a4034`. PoC in `ipv6/`: `ipv6/run.sh` and `ipv6/copyfail2v6.c`. Uses `::1` loopback and `ip -6 xfrm`. ESP packet padded to >= 40 bytes to clear the `xfrm6_input.c:124` size gate.

Credits

Hyunwoo Kim (imv4bel) and Kuan-Ting Chen reported, tested, authored the upstream fix.

About

Copy Fail 2: Electric Boogaloo

Readme
Activity
203 stars
9 watching
17 forks
Report repository

Releases

No releases published

Packages

No packages published

Contributors 2

0xdeadbeefnetwork _SiCk
sickthecat Sick the Cat

Languages

C 62.0% **Shell** 38.0%

Steffen Klassert: IPsec maintainer, posted the fix to netdev/net.git.

Brad Spengler (@spendergrsec / grsecurity): called it copyfail-class before anyone else read the commit.

Theori / Xint: original Copy Fail (CVE-2026-31431).