New issue

mkfifo TOCTOU race via path-based chmod #10020

Open #10052

Labels U - mkfifo good first issue reported-canonical

sylvestre opened on Jan 3 Contributor

Component

`mkfifo`

Description

mkfifo creates a FIFO and then unconditionally performs a path-based `chmod` via `std::fs::set_permissions`.

Between these operations, an attacker with write access to the containing directory can replace the FIFO with a symlink.

Additionally, for the default case (no `-m` flag), the chmod is redundant as the kernel already applies umask during creation.

Test / Reproduction Steps

```
# Terminal 1 (attacker, racing the chmod):
while true; do
  rm -f /tmp/fifo; ln -s /etc/shadow /tmp/fifo
done

# Terminal 2 (victim with privileges):
while true; do
  rm -f /tmp/fifo; mkfifo -m 0666 /tmp/fifo
done
```

```
# Check if /etc/shadow permissions changed
```

sylvestre added **U - mkfifo** **good first issue** on Jan 3

aristarhoskal linked a pull request that will close this issue on Jan 4

mkfifo: Fix path-based chmod race #10020 #10052

sylvestre added **reported-canonical** on Jan 17

Metadata

Assignees

No one assigned

Labels

U - mkfifo **good first issue** **reported-canonical**

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

mkfifo: Fix path-based chmod race #10020

uutils/coreutils

Participants