Attack of the setuid bit

pt_chown and pwning root terminals

Siddhesh Poyarekar

Toolchain Engineer, Red Hat

13-Feb-2014

Agenda

The Problem summary

Using a setuid root program called `pt_chown`, one may get ownership of another user's pseudo-terminal file by using a 'feature' available in FUSE.

Overview of the Login Process

- The pseudo-terminal file
- devpts
- The `grantpt()` function
- `pt_chown`

Overview of FUSE

- Filesystem in userspace
  - Userspace programs
  - Callbacks for primitives
  - Limited ioctl support
- The `user_allow_other` option

Pre-Conditions

- Kernel with FUSE and ioctl support
- `user_allow_other` enabled in `/etc/fuse.conf`
- The victim user logged in and has a pseudo-terminal file in `/dev/pts/`

The Attack in Action

- An empty directory to act as a mount point
- Mount the fake filesystem
- Open a dummy file in the filesystem as file descriptor 3
- Execute textttpt_chown
- `pt_chown` calls `ptsname()` for fd 3, which calls `isatty()`...
  - Fooled by `TCGETS` into believing that it is!
- ptsname() gets the terminal number for the fd...
  - Fooled by `TIOCGPTN` into thinking that it is `/dev/pts/number-you-gave`!
- Pseudo-terminal pwned!

The Fix

Remove pt_chown from installations

- Useless since the introduction of devpts
- Only a fallback for incorrect configurations

Other Issues

- Alternative fix: `isatty()` doesn't check the termios structure
- Misusing ioctls in FUSE

Credits

- **Martin Carpenter** (http://mcarpenter.org/blog/) found and reported the vulnerability
- **Carlos O'Donell, Roland McGrath, Joseph Myers, Andreas Schwab and Andreas Jaeger** for their reviews and insights on the problem.

Questions?