Kernel Exploit Walk-through: CVE-2017-7038

or

“Thank you Andrey Konovalov for developing and explaining your kernel exploits”

OSU Security Club, Mar 7, 2019

Kees (“Case”) Cook
@kees_cook
keescook@chromium.org kees@outflux.net

https://outflux.net/slides/2019/osu/walkthru.pdf

About me

- Employed by Google, focusing on upstream Linux kernel security defenses
  - work closely with Chrome OS, Android, and Cloud
  - member of upstream kernel security response team
  - member of upstream kernel Technical Advisory Board
- Kernel Self-Protection Project
  - Remove bug classes
  - Eliminate exploitation methods

References for this presentation

- https://github.com/xairy/linux-kernel-exploitation
- https://googleprojectzero.blogspot.com/2017/05/exploiting-linux-kernel-via-packet.html
  - https://github.com/xairy/kernel-exploits/tree/master/CVE-2017-7308
  - https://github.com/torvalds/linux/commit/2b6867c2ce76c596676bec7d2d525af525fdc6e2
- https://launchpad.net/ubuntu/+source/linux-hwe/+publishinghistory
  - https://launchpad.net/~canonical-kernel-security-team/+archive/ubuntu/ppa/+build/12081046
- https://syzkaller.appspot.com
  - https://github.com/google/syzkaller/blob/master/docs/linux/setup_ubuntu-host_qemu-vm_x86-64-kernel.md

Exploit Prep

- `git clone https://github.com/xairy/kernel-exploits.git`
- `cd kernel-exploits/CVE-2017-7308`
- `make poc`
- `cd -`

Kernel Prep

- `mkdir ubuntu`
- `cd ubuntu`
- `wget https://launchpad.net/~canonical-kernel-security-team/+archive/ubuntu/ppa/+build/12081046/+files/linux-image-4.8.0-41-generic_4.8.0-41.44~16.04.1_amd64.deb`
- `dpkg-deb -x linux-image*deb .`
  - `ar p linux-image*deb data.tar.bz2 | tar jx`
- `cd -`

Target Prep

- Either grab a copy of the image here:
  - https://outflux.net/nx/stretch.img.xz

- or follow along in the next slides...

Target Prep (1 of 2)

- `git clone https://github.com/google/syzkaller.git`
- `mkdir target`
- `cd target`
- `../syzkaller/tools/create-image.sh`
- `sudo mkdir -p /mnt/chroot`
- `sudo mount -o loop stretch.img /mnt/chroot`
- `sudo chroot /mnt/chroot apt install net-tools`

Target Prep (2 of 2)

- `sudo chroot /mnt/chroot adduser user`
- `sudo cp -a ../kernel-exploits/CVE-2017-7308/poc /mnt/chroot/home/user/`
- `sudo cp -a ubuntu/lib/modules /mnt/chroot/lib/`
- `sudo chroot /mnt/chroot depmod -a 4.8.0-41-generic`
- `sudo umount /mnt/chroot`

Run VM

-
  ```
  qemu-system-x86_64 \
    -kernel ubuntu/boot/vmlinuz* \
    -append "console=ttyS0 root=/dev/sda debug earlyprintk=serial" \
    -hda stretch.img \
    -net user,hostfwd=tcp::10021-:22 -net nic \
    -enable-kvm -cpu host -smp 2 -m 2G \
    -nographic \
    -pidfile vm.pid \
    2>&1 | tee vm.log
  ```

Run Exploit

- *press enter*
- `su - user`
- `./poc`
- `id`

- When you exit the poc, the kernel will likely hang, so kill the VM:
  - `ps -ef | grep qemu`
  - `kill` *PID*

Let’s walk through the write-up for what just happened ...

- https://googleprojectzero.blogspot.com/2017/05/exploiting-linux-kernel-via-packet.html

Mitigations

- `echo 0 > /proc/sys/user/max_user_namespaces`

- removal of memory position report, %p hashing
- struct timer refactoring
- cr4 pinning

- Future: XPFO, integer overflow detection