Android 0dayz hunting

Why rooting ?

- For fun !
- For profit !
  - “Jailbreak”
  - Forensics acquisition
  - Bad evil malware

Targets

- Low hanging fruits !
- Rump 2012: command injection in netd (Net daemon running as root)
- Other 90's vulns in core ?

Of course!

- Android 4.4.3 pushed to AOSP
- Changelog:
  - Project: platform/system/vold
  - 0de7c61 : Validate asec names

ASEC

```
snprintf(asecFileName, sizeof(asecFileName),
                  "%s/%s.asec", asecDir, id);

snprintf(mountPoint, sizeof(mountPoint),
                  "%s/%s", Volume::ASECDIR, id);
```

- “id” user controlled
- What about a nice cup of “../” ?

Exploitation

- Id ← “../../../../data/local/tmp/xxx”
  - ASEC file created in /data/local/tmp/xxx.asec
  - Mounted in /data/local/tmp/xxx

- If /data/local/tmp/xxx exists AND is a symlink ?
  - Symlink followed, container can be mounted in any directory (“/system/bin”, “/sbin”, …)
  - Container's content is of course user controlled

Requirements

- “shell” user (via adb)
- Application with ASEC_* permissions
  - Not so common

Old vuln ?

- Introduced in 2010 with ASEC support
- Patched in Android 4.3.3 (2014)
- Known by at least one mobile forensics editor
  - For at least 2 years !

</android>

More details on the vulnerability:
http://blog.cassidiancybersecurity.com

IDA 6.6 is out \o/