OpenAFS Status 2015
The final countdown

- Daria Phoebe Brashear
- The OpenAFS Project

- 19 August 2015

What are you running?

- Folks here running previous-to-1.6.5
  - and before 1.6.5, you are vulnerable
  - there are also issues, albeit less severe, up to 1.6.12

OpenAFS 1.6.13

- Security release
  - Several pent-up security issues addressed
  - One patch caused problems with backup software
    - disabling regular expression (regex) support in the vlserver for gathering lists of volumes by attribute broke the inboard backup system as well as TSM

OpenAFS 1.6.14

- Buffer length limit for regular expression handling to prevent trivial denial of service.
- But attribute listing made an operation requiring privilege to protect against other abuses.

vos client stack data leak

- vos allocates new vldb entry storage from the stack
  - Buffer was not cleared before use, meaning stack contents could be leaked onto the wire
  - vos by default would send this info in the clear

bos vulnerable to command spoofing

- bosserver did not require encrypted commands
- rxkad “auth” mode does not integrity-protect the message payload
- A legitimate RPC could be tampered with to perform undesired changes, including modifications
- bos changed to default to encrypting
- bosserver requires encryption

bos vulnerable to command spoofing

- bosserver did not require encrypted commands
- rxkad “auth” mode does not integrity-protect the message payload
- A legitimate RPC could be tampered with to perform undesired changes, including modifications
- bos changed to default to encrypting
- bosserver requires encryption

vlserver regular expression support

- VL_ListAttributesN2 RPC
  - used to collect lists of volumes
- Buffer overflow possible
- Attempting to allocate infinite resources also possible
- disabled in 1.6.13
- fixed and restricted in 1.6.14

pioctl kernel memory contents leak

- pioctl is the userspace/kernelspace mechanism for I/O
- Buffers reused from pool without being cleared
- Fixed to clear buffers before use

OSD support could panic kernel

- AFS/OSD included a means to proxy commands to a fileserver
- Returned data was written to an incorrect location
- Likely result was a kernel panic
- Fixed to return correctly.

Solaris PAG handling may panic

- The check for overflowing the group list with the 2 groups for a PAG was done improperly
  - A buffer for the modified group list was possibly also not large enough.
  - Small overwrite might not cause a panic, but not good.
  - Caught errors would cause a deadlock.
  - Fixed to check bounds.

MacOS issues

- binary signing
  - kext signing required in 10.10
  - neither packaging nor binaries are signed
  - and the current packaging can’t be signed
  - YFS has downloadable signed packages
  - more on this tomorrow

Windows

- Key signing makes this ridiculously complicated
- We'll talk more about it tomorrow.

OpenAFS 1.6.14.1

- Linux kernel support
  - support for Linux 4.2
  - only use automount for volume roots
    - a fix for the dentry alias issue which still works with Linux 4.2

Other work

- Restricted Query (avoid leaking metadata) patch
- Issue is things like volume names and pts identities "leak" the existence of usernames
  - Privacy concerns

Other work

- volscan work
  - alternate mode of use for volinfo tool
  - can be used to generate statistics about data by server, partition, volume, volumetype, or other metrics

Next Release Series

- 1.8? What's what??
  - Still working on what will be coming in and what will stay on master

Talk back to us

- Mailing lists:
  - Openafs-info http://lists.openafs.org/mailman/listinfo/openafs-info
  - Openafs-devel http://lists.openafs.org/mailman/listinfo/openafs-devel
  - Foundation-discuss http://lists.openafs.org/mailman/listinfo/foundation-discuss
- IRC chat room: #openafs on freenode
- Jabber developer MUC: openafs@conference.openafs.org