Improving the FreeBSD security advisory process

Philip Paeps
14 January 2020
Linux.conf.au 2020
Gold Coast, QLD, Australia
FreeBSD is an open source Unix-like operating system descended from patches developed at the University of California, Berkeley in the 1970s.

The FreeBSD Project is an active open source community since 1993 with hundreds of committers and thousands of contributors around the world.

The FreeBSD Foundation is a non-profit organisation registered in Colorado, USA in 2001 dedicated to supporting the FreeBSD Project, its development and its community.
Who uses FreeBSD?
Where FreeBSD excels

Community
- Friendly and professional
- Many active contributors and committers for 10+ and even 20+ years (and longer)

Mentoring
- Built into the Project’s culture and processes

Documentation

Licence
- 2-clause BSD licence
- Does not restrict what you can do with your own code!
Where FreeBSD (historically) doesn’t excel

**Security**

- Timely handling of security vulnerabilities
Large and diverse code base

**Kernel**
- Networking
- Storage
- Device drivers
- Virtual memory

**Userland**
- Libraries
- Applications

**Third-party base components**
- OpenSSL
- OpenSSH
- Sendmail
- Unbound
- ntpd

**Ports / packages**
- 35,000+ third-party applications
Vulnerability response

FreeBSD only response

• No NDA or explicit embargo
• Only applies to FreeBSD (and maybe to NetBSD and/or to OpenBSD)
• No major risk of exposure

Examples
  • SA-18:04.vt
  • SA-17:10.kldstat

Multi-vendor coordinated response

• NDA and/or explicit embargo
• Coordinated response via private party or CERT/CC
• Requires limited disclosure to contain risk of exposure

Examples
  • SA-18:03.speculative_execution
  • SA-18:06.debugreg
Security officer charter

- Resolving disputes involving security
- Resolving software bugs that affect the security of FreeBSD in a timely fashion
- Issuing security advisories for FreeBSD
- Responding to vendor inquiries regarding security issues
- Auditing as much code as possible
- Monitoring the appropriate channels for reports of bugs, exploits, and other circumstances that may affect the security of a FreeBSD system
- Participating in the architecture of FreeBSD in order to influence a positive impact on system security
- Maintains the FreeBSD Security Officer PGP key
Challenges facing the security team

• Extremely broad mandate
• A lot of hurry up and wait activities not conducive to a friendly employment environment
• Very high level of very technical knowledge required to respond to the large variety of issues
Results of challenges

- Burn out
- Few qualified candidates have level of knowledge required to do the job
How we are fixing it

• New blood
• Splitting the technical resource requirement from the vulnerability response requirement
• Allows us to use non-technical resources for the vulnerability response while technical resources only need to focus on the technical response
FreeBSD Foundation involvement

• Holder of NDA and vendor relationships
  • Survivability of changeover of security officer
  • Vendor relationships

• Funds resources
  • Pays for the deputy security officer’s time
  • Pays for the security officer’s travel
  • Pays for development resources to enable response (one full time employee)
Case study: CVE-2018-8897 / SA-18:06.debugreg

• CVE-2018-8897 was a multi-vendor response which FreeBSD was pulled into early in the coordinated response process by Microsoft
• Included representations from the BSDs, Microsoft, Apple, Citrix, VMWare, Linux distros, Google, and Intel
• Lots of collaboration on PoCs and fixes with other BSD variants
• Once CERT/CC was involved, we were able to give pre-embargo patches to pfSense
• Published SA within one hour of drop of embargo
• We beat RedHat 😊