15+ years of oss-security

A talk by

Solar Designer <solar@openwall.com>
@solardiz

@Openwall / https://www.openwall.com

@Binarly_io / https://binarly.io

June 2023

15+ years of oss-security

Timeline

```
1980----------------1990----------------2000----------------2010------------>

Usenet net.unix-wizards   Bugtraq         Vulnwatch     oss-security
{alt,comp}.security.*     1993 - 2020     2001 - 2008   2008 - present
1980s - 2000s                               full-disclosure
                                            2002 - present

        Security Mail List        vendor-sec                  (linux-)distros
        1984 - 1989               1997 - 2011                 2011 - present
                  Zardoz
                  1989 - 1991

                CERT/CC                                 oCERT
                1988 - present                          2008 - 2017
```

Disclosure debate

- "As far back as the 19th century, we had Locksmiths trying to figure out how to reasonably disclose weaknesses in locks" (Haroon Meer, 2015)

- Non-disclosure

- Responsible disclosure
  - Unnecessarily judgmental term, as if any other option were irresponsible

- Full disclosure

- Security holes are just bugs
  - "security holes in Unix should be treated like any other bug and reported" (opinion mentioned in the very first "Security Mail List" posting, 1984)
  - "[...] "disclosing" is the fixing of the bug" (Linus Torvalds, 2008)

Introducing oss-security

* Started in 2008 due to prodding by Josh Bressers
  + Purposefully independent from any major distro vendor

* Public mailing list (and wiki) focused on Open Source software security
  + Bugtraq and full-disclosure were not focused
  + vendor-sec was not public

* Added private mailing list(s) (linux-)distros in 2011
  + vendor-sec ceased to exist and (arguably) needed a replacement

* linux-distros reaches Linux distros and list admin only
  + Currently 17 Linux distros and Openwall in list admin capacity
* distros reaches all members
  + linux-distros and currently also FreeBSD, NetBSD/pkgsrc, Oracle Solaris

15+ years of oss-security

Public list: oss-security

* Messages must be on Open Source software security, helpful for the community
* Security advisories aimed at end-users only (by distros) are not welcome
* Content quality guidelines (informative Subjects, self-contained messages)
* Linux not implied, other Open Source operating systems are first-class too

* Anyone can subscribe
* Anyone can post
  + No subscription required (but it's preferable to subscribe)
  + Most messages are pre-moderated (thanks to Henri Salo, the co-moderator)
    + Moderation delays are low compared to Bugtraq's
    + Rejection rate is very low (not counting automated spam)
* Currently about 100 messages per month (after spam filter and moderation)
  + 28800+ messages in 15+ years so far (average over 150 per month, peak 485)
  + For some years, CVEs could be requested via the list, inflating traffic

15+ years of oss-security

Private list: (linux-)distros

* Messages must be on Open Source software vulnerabilities that are non-public
  + Likely actionable within 14 days for some member distros
* Linux-specific issues should be sent to the linux-distros sub-list
  + Not to spam nor unnecessarily disclose them to the non-Linux members

* Only Open Source operating system vendors meeting criteria can subscribe
  + Requests must be made and are discussed in public on oss-security
* Anyone can post
  + By posting, the issue reporter accepts certain responsibilities
    + Must propose a public disclosure date/time (within 14 days)
    + Must post to oss-security on the day the issue is (to become) public
    + If exploit(s) were shared, must post them to oss-security too
    + May optionally delay that by up to another 7 days
* Once the issue is public, any follow-ups belong on oss-security (not distros)

Semi-public issues

There are two kinds:

* Explicit public pre-notification of upcoming full disclosure - usually OK
  + Very limited information (e.g., severity and planned disclosure date)
  + OpenSSL and Exim do this
    + Fit (linux-)distros policy as-is

* Publicly discussed and/or committed silent fix - often problematic
  + Level of detail varies, sometimes security relevance can be inferred
  + Linux kernel and curl do this, differently
    + Added exceptions to accommodate their development/testing processes
  + For other projects, exceptions may be granted on a case-by-case basis

Current (linux-)distros members

* distros
  + All who are also on the linux-distros list below
  + FreeBSD, NetBSD/pkgsrc, Oracle Solaris

* linux-distros
  + ALT Linux, Amazon Linux, Arch Linux, Chrome OS, CloudLinux, Container-Optimized OS (COS), Debian, Flatcar Container Linux, Gentoo, Microsoft Linux Systems Group, Oracle, Red Hat, Slackware, SUSE, Ubuntu, VMware Photon OS, Wind River
  + Openwall as list admin

* Never send a message to both lists at once (choose the appropriate one)
  + Note that distros also includes linux-distros, so reaches all of the above

(linux-)distros membership criteria and rules in a nutshell

* Be a maintained distro with substantial use of Open Source components
* Have a userbase not limited to your own organization
* Show that your membership during the recent year would have helped the users
* Not be only downstream or rebuild of another distro (exceptions possible)
* Be a participant and preferably a contributor in relevant public communities
  + Especially on oss-security
* Accept the list policy (handling of the information on a need-to-know basis)
* Be able and willing to contribute back in specific ways announced in advance
  + We have a lengthy list of contributing-back tasks currently including 6 technical (such as code reviews and testing) and 16 administrative ones
  + Many are already taken and handled, some not fully handled, some vacant
* Be able and willing to handle PGP-encrypted e-mail
  + All messages via the list are encrypted to the individual recipients' keys
* Have someone already on the list or active on oss-security vouch for you

(linux-)distros statistics

* One of the larger contributing-back tasks that isn't currently handled is keeping track of issue handling and disclosure timelines and sharing with the public of the raw data and computed statistics
* This is important not only for transparency, but also to see how we're doing and what we can improve, and even more importantly to detect any failures to meet the maximum embargo time promptly
* Gentoo was handling this task well since mid-2017 until September 2019
* Amazon Linux tried to retroactively automate it for 2022, but that missed and mixed up many data points - indeed, the input data isn't formalized
* Per statistics produced by Gentoo:
  + In 18 months since mid-2017 until end of 2018, we handled 161 issues with average and median embargo duration of about 6 days
  + In 9 months since January to September 2019, we handled 49 issues with per-month average and median embargo duration from 3 to 9 days

15+ years of oss-security

Volunteer or funded effort?

* In the 15+ years so far, Openwall received no funding to run the lists, so this was a 100% volunteer effort
* It's unlikely that any of the member distros received external funding in connection with their membership and contributing-back tasks either
  + However, many are large companies that presumably allow or ideally encourage their employees to spend paid work time on these tasks

* An option could have been to request membership dues and use the funds to handle all of the tasks consistently
  + However, we deliberately did not - that would have been controversial, inconsistent with prior practice (e.g., vendor-sec and CERT/CC), and discriminatory against smaller/community distros (we'd need an exception)
  + The current non-monetary contributing-back model has community spirit
* Potential funding by the Linux Foundation is currently under consideration

Potential evangelism - help wanted

* Monitor for Open Source security issues/topics published elsewhere, identify which of these would fit, and bring them to oss-security
* Directly encourage upstreams, researchers, umbrella organizations, packagers, distros, etc. to report to the lists
* Suggest and provide examples of quality improvements for such reports
* To make oss-security more self-contained, post follow-ups adding detail that was previously only available via external links
* Consider developing tools to help with the above (crawl URLs in messages and produce draft follow-ups for manual editing+posting)

* More reliable oss-security Twitter/Mastodon feed(s)
  + The existing Twitter feed occasionally misses messages
* New curated "best of oss-security" Twitter/Mastodon feed(s)

15+ years of oss-security

Opinionated observations

* Fixing bugs is important, but attack surface reduction, defense-in-depth, and even anti-exploitation mitigations may be more important

* (linux-)distros membership criteria, encryption, secure operation are important, but the 14 days maximum on embargo duration is more important

* Semi-public silent fixes are problematic, but Linux kernel's growing attack surface is more problematic

* Most of the Linux kernel issues brought to linux-distros are an arbitrary subset of the many more issues being discovered by fuzzing - why bother?
  + However, occasional well-researched higher-severity exceptions exist

* Reports against userland code are of higher quality on average

Mailing lists vs. modern e-mail security

* Mailing lists resend messages from their servers, which can violate SPF
  + Unless sender address is changed to the list's
    + Normally done for envelope-from (SMTP "MAIL FROM:"), not always enough
    + Inconvenient to also do for header From (breaks replying to person)

* Mailing lists change headers (add list prefix) and/or bodies (encrypt)
  + Breaks DKIM

* With the sender domain's DMARC set to p=reject, some recipients don't get the messages (most notably, those on Google mail servers)
* For posting to lists, please use your (sub-)domain without such setting

* No perfect solution, so will have to be adding problematic workarounds

15+ years of oss-security

Contact information

oss-security list archive
https://www.openwall.com/lists/oss-security/

Detailed instructions, how to subscribe, how to post
https://oss-security.openwall.org/wiki/mailing-lists

e-mail
Solar Designer <solar@openwall.com>

Twitter
@solardiz @Openwall

website
https://www.openwall.com