Adventures in Software Security Defect Management

UKNOF36 - Cathy Almond, ISC

© 2017 ISC

Adventures in Software Security Vulnerability Management

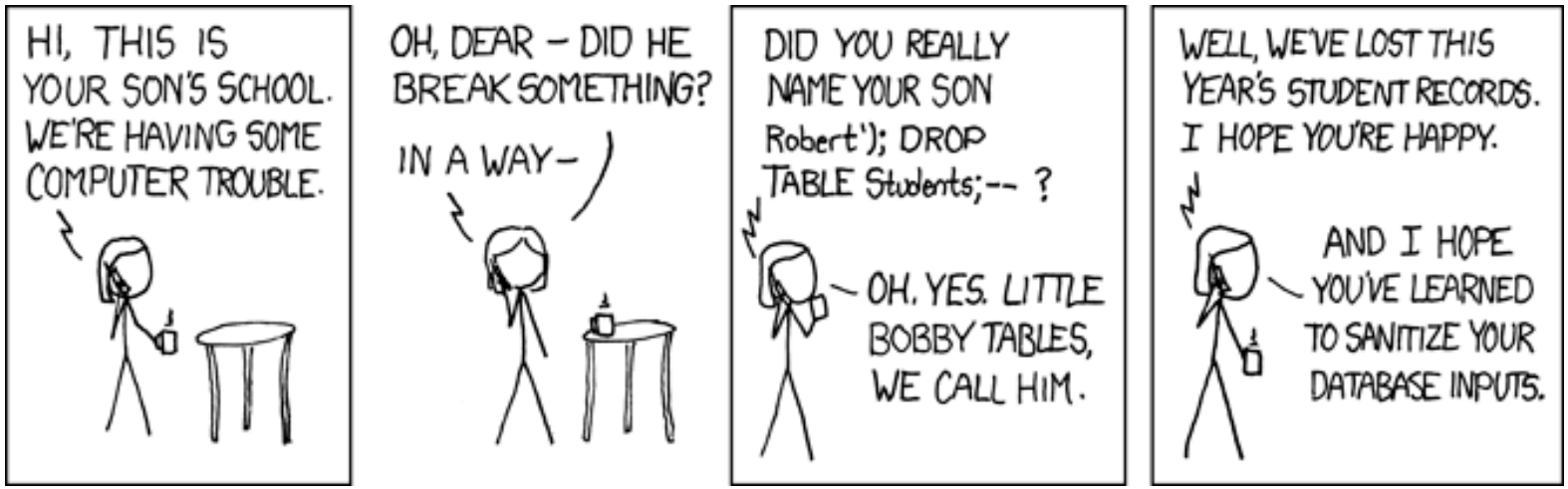
"QA Engineer walks into a bar. Orders a beer. Orders 0 beers. Orders 999999999 beers. Orders a lizard. Orders -1 beers. Orders a sfdeljknesv..."

https://twitter.com/sempf/status/514473420277694465

© 2017 ISC

There are some bugs…

- All (non-trivial) software has bugs
- Testing isn't infallible
- It might not be your QA guy ordering those beers

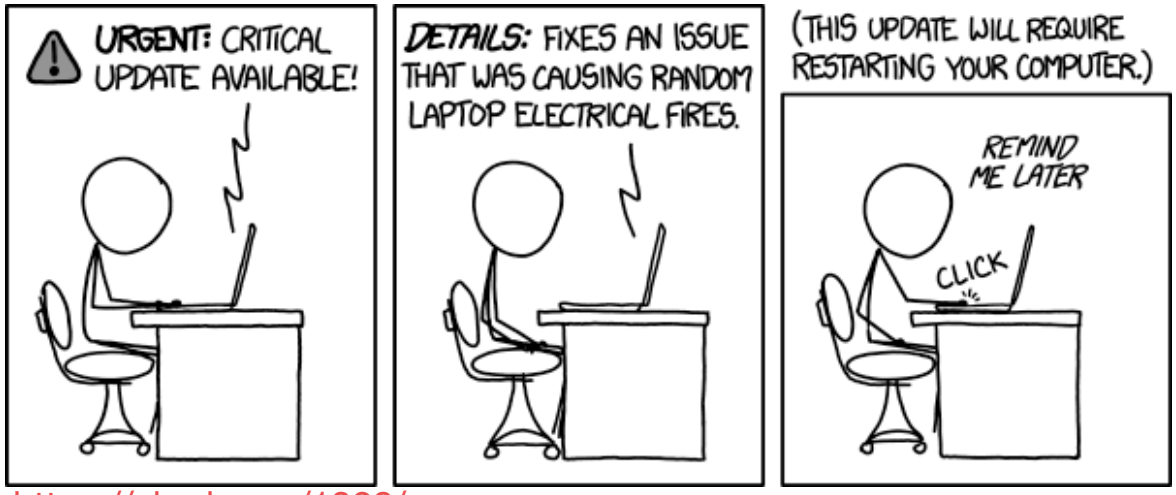


https://xkcd.com/327/

© 2017 ISC

…that we have to fix

- Release before someone else finds it?
- Postpone because…?
- Adopt a ‘batching’ policy – e.g. ‘first Wednesday is always patch day’?



https://xkcd.com/1328/

© 2017 ISC

More bugs than ever before?

- Google's 'bounty' programs inspired a new generation of bug hunters: https://www.google.com/about/appsecurity/patch-rewards/index.html
- We improved our own testing techniques (e.g. 'fuzzing': http://lcamtuf.coredump.cx/afl/) and are finding more bugs ourselves in-house.
- Not all, but a majority of vulnerabilities have lain undiscovered for many years – better testing is the reason for the increase in announced vulnerabilities, not deteriorating code quality

© 2017 ISC

Best Practices

There are plenty of policies and guidance documents out there – handling security vulnerabilities should be a mature business process:

- http://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip
- https://www.isc.org/downloads/software-support-policy/security-advisory/
- https://www.first.org/cvss *(we're using CVSS v3.0)*

But some decisions are still hard…

© 2017 ISC

What would you do if...?

1. You're just about to release a new beta version of your product, and a security defect is uncovered. Release anyway, fix in final?
2. What if it's the final production-ready version due tomorrow with parties, fireworks etc.. Release anyway, plan to patch soon?
3. What if the bug has lain undiscovered in the code for 10+ years, so all other released versions are already vulnerable?
4. What if the bug would only affect a very small subset of users (e.g. a niche feature)?

© 2017 ISC

What would you do if…?

5. You suspect there might be other bugs of similar ilk/mechanism waiting to be found and you want to test more thoroughly before releasing any fixes/announcements?
6. Announcing this defect today might inspire external malicious bug-hunters to start looking for other vulnerabilities now too?
7. It's nearly the holidays… ?
8. This the third bug in as many months and your consumers are weary of upgrading?

© 2017 ISC

Who might you tell?

- The Internet ‘public’ (non-paying consumers)
- Other organisations who repackage/distribute your software in their OS/appliance/device
- Core Internet Infrastructure providers
- Paying customers
- CSIRTs and other security coordination organisations
- Nobody who hasn’t signed a non-disclosure agreement?

© 2017 ISC

Is it ‘right’ to..?

1. Sell early-release security issue details/fixes?
2. Notify OS packagers (for no fee) ahead of publicly announcing a vulnerability?
3. Tell anyone at all in advance without a signed non-disclosure agreement between us and them?
4. Distribute details on how to test/demonstrate the defect when announcing the defect/fixes?
5. Bundle all security fixes to a pre-announced default monthly or quarterly date?

© 2017 ISC

Important note:

ISC released 4 BIND security advisories on 11th January 2017:
https://www.isc.org/downloads/software-support-policy/security-advisory/

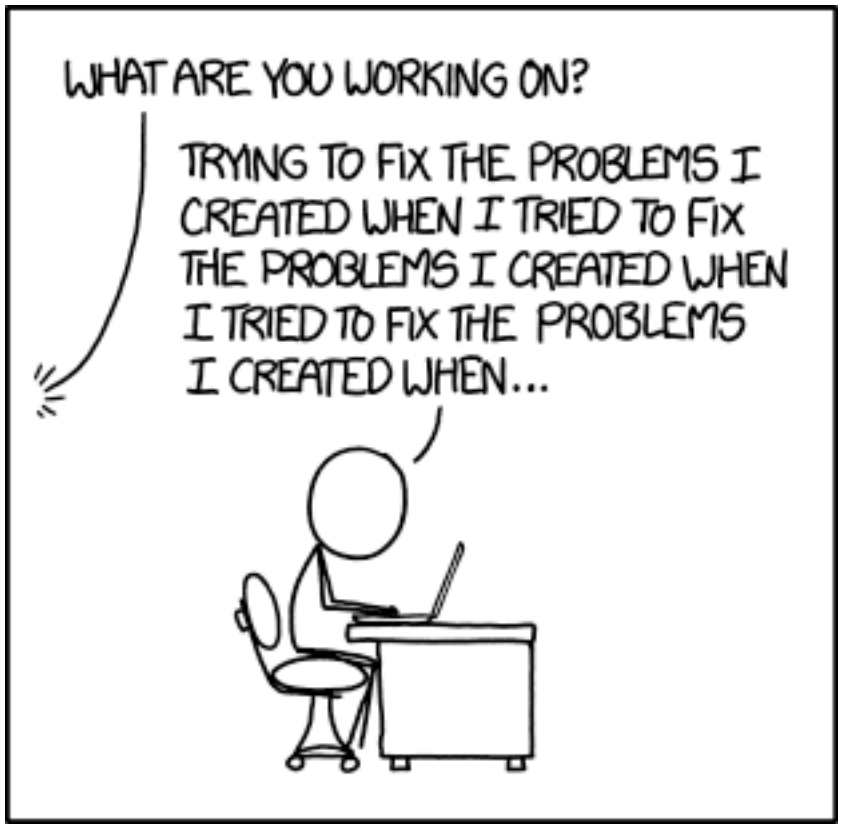
- Downloads: https://www.isc.org/downloads/
- Mailing list (sign-up): https://lists.isc.org/mailman/listinfo/bind-announce
- Subscribe to the KB (email or RSS): https://kb.isc.org/category/74/0/10/Software-Products/BIND9/Security-Advisories/

© 2017 ISC

P.S.

- *We deferred our beta releases (we didn't want to release new code with known vulnerabilities).*
- *We deferred announcing the first bug found using our newest angle on testing, anticipating others (two more – a customer found the fourth).*
- *We do notify OS packagers ahead of the public announcements.*
- *We do sell an early notification/patches service; Open Source is free to use and download and this is one way whereby we can fund its on-going maintenance and development.*

© 2017 ISC



ANY QUESTIONS?

https://www.isc.org/downloads/software-support-policy/security-advisory/

© 2017 ISC