The GNOME™ Conference

GUADEC

What's Coverity static analysis ever done for us?

Philip Withnall
Endless Mobile
philip@tecnocode.co.uk

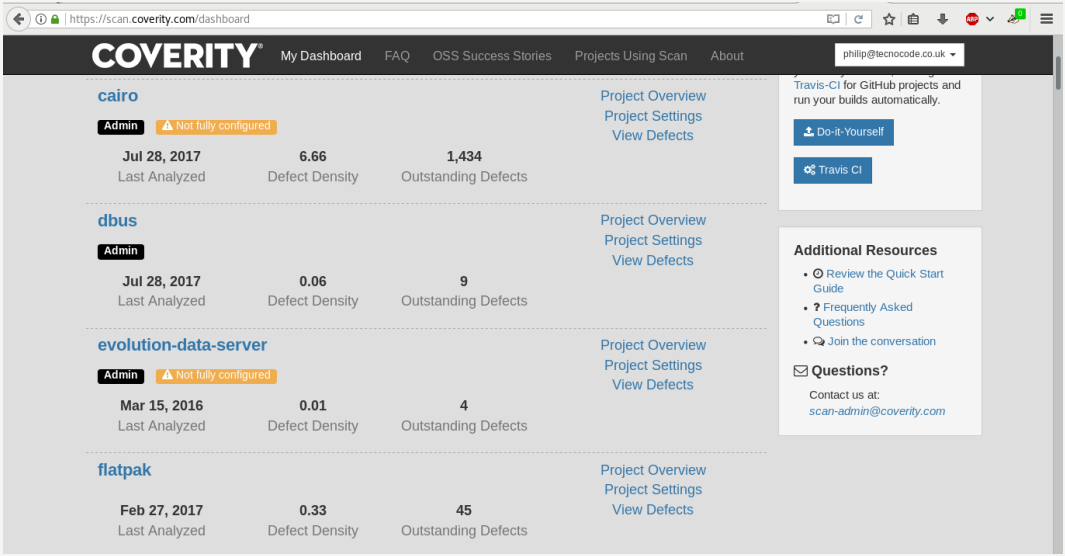
What is static analysis?

Compile-time testing of all possible code paths.

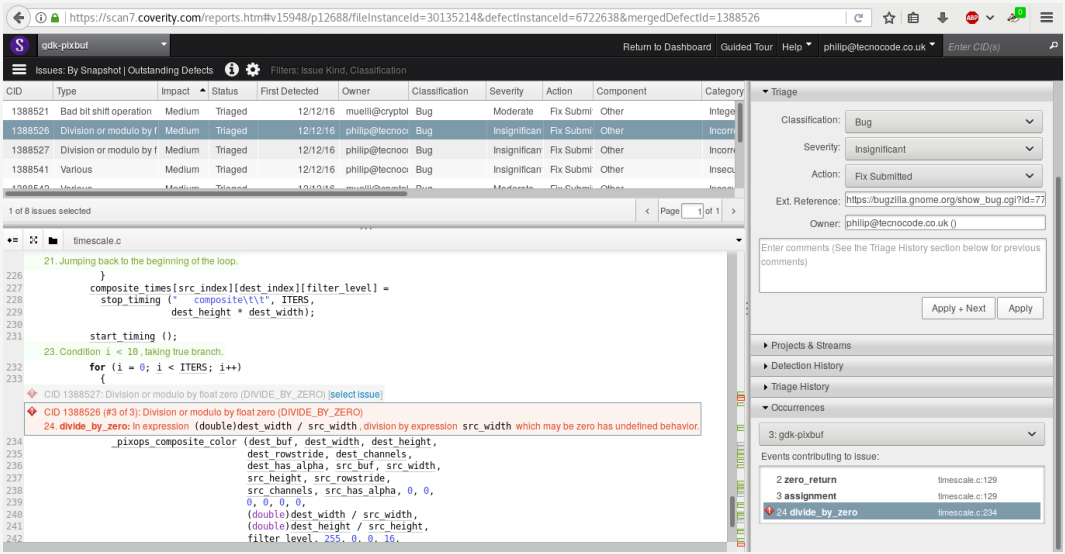
What is Coverity Scan?

- Proprietary
- Free to use for open source projects
- A locally run tool and paired web service

What is Coverity Scan?



What is Coverity Scan?



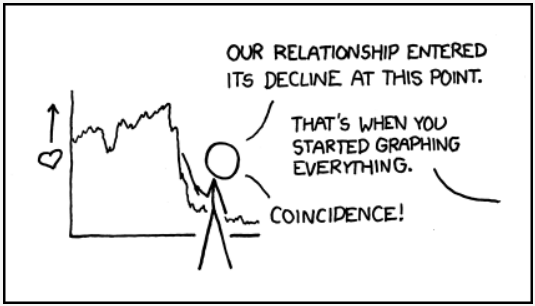
Is it the best tool for the job?

- Mature support for triaging and dismissing false positives
- Wide use over many projects and active development
- Free to use
- Proprietary
- Submission rate limiting
- Should be used as one tool out of many

How have we been using Coverity?

- Jenkins + JHBuild
- Manually created Jenkins jobs
- Limited set of hand-picked ‘security critical’ modules
- E-mail notification of scan results
- Partial ownership by module maintainers
- No real comaintainership of the project

What impact has this had?



Randall Munroe, `https://xkcd.com/523/`, CC-BY-NC 2.5

How is this useful?

- Find bugs in error paths
- Complements unit testing
- Find bugs in parsers and file loaders
- Find bugs before they are hit at runtime
- Jenkins won't forget to run analyses like maintainers do

How is this not useful?

- Not reasonable to use as a try-server
- Initial dump of false positives when adding a project
- Problems with handling idiomatic C
- Jenkins + JHBuild is not the most reliable

How do I get involved?

- Talk to me; propose modules for inclusion into Jenkins
- Or go with Coverity yourself
- Or try other static analysis tools (`clang-analyzer`?) and let me know!

Miscellany

Jenkins jobs `https://jenkins.freedesktop.org/view/GNOME%20Coverity/`

Coverity `http://scan.coverity.com/`

Wikipedia on static analysis
`https://en.wikipedia.org/wiki/Static_program_analysis`

Beamer theme: `https://git.gnome.org/browse/presentation-templates/tree/GUADEC/2017`