Don’t Ignore GitHub Security Alerts, Automate Them Into Your Workflow.

Verizon Media

March 13, 2019
Quick Intro

Ashley Wolf
Open Source Program Manager
Verizon Media

Yahoo Open Source

Twitter: @Meta_Ashley
Verizon Media Open Source Program Office

7K
All engineering employees benefit from OSPO services

330
Support tickets quarterly

440
Active Open Source Projects published by Verizon Media

25
GitHub organizations that we manage

200+
Mobile and TV Applications that rely upon our services for compliance
What does an OSPO do?

**Program Management**
Supporting internal engineering groups with open source issues

**License inbound review**
Reviewing the use of open source in our products and platforms

**Contributions to projects**
Reviewing contribution policies and CLAs

**Compliance Management**
Responsible for mobile and TV app compliance engineering and automation

**Community development**
Promoting projects via blogs, podcasts, and speaking events

**New project publication**
Reviewing publication steps completed prior to publication

**Issue support and resolution**
Ensuring issues are addressed on our external repos

**Security Alerts**
GitHub alerting us about vulnerable dependencies
What’s an information security issue to an OSPO?
InfoSec people care about production issues

Bug Bounty
Code Scanning
Red/Blue teams, etc.
We’re talking about vulnerabilities that are in a published piece of code.
OSPOs need to care about security issues in their published code.
Good News, Bad News

GitHub can help

It’s limited and not designed for OSPOs, only for project owners.
Agenda

- What GitHub does to help your companies’ open source security issues
- Where the alerts and APIs fall short
- A call for you to help develop a better solution
GitHub Provides Security Alerts
GitHub Security Alerts

Dependency graph

We found a potential security vulnerability in one of your dependencies.

The `actionview` dependency defined in `Gemfile.lock` has a known moderate severity security vulnerability in version range `>=4.0.8, <=4.2.7` and should be updated.

Only users who have been granted access to vulnerability alerts for this repository can see this message.

Learn more about vulnerability alerts

These dependencies have been defined in `VulnerabilityTestRepoRubyGems`'s manifest files, such as `Gemfile` and `Gemfile.lock`
The vast majority (81%) of vulnerable dependencies may be fixed by simply updating to a new version

GitHub Email Alerts

AshleyWolf,

We found a potential security vulnerability in a repository for which you have been granted security alert access.

**Project**: yahoo/artifactory_ssh_proxy

Known **high severity** security vulnerability detected in

`com.fasterxml.jackson.core:jackson-databind < 2.6.7.1` defined in

`pom.xml`.

`pom.xml` update suggested: `com.fasterxml.jackson.core:jackson-databind ~> 2.6.7.1`.

Always verify the validity and compatibility of suggestions with your codebase.

[Review vulnerable dependency](#)
Some of the problems that OSPOs will have

- Opt-in only for private repos
- Vulnerability Alerts API cannot turn on notifications
- Email give you only 10 repos in daily digest
- Not all project languages supported
- No dashboard of alerts including notification dismissal reasons
- Not automated!
e.g.: The project owner ignores issues
Automating Security Workflow Project
Automate Security Workflow
Automating the Alert Workflow

GitHub

ashleywolf,

We found a potential security vulnerability in a repository for which you have been granted security alert access.

feeds/yahoo/artifactory_ssh_proxy

Known high severity security vulnerability detected in com.fasterxml.jackson.core:jackson-databind < 2.6.7.1 defined in pom.xml.

pom.xml update suggested: com.fasterxml.jackson.core:jackson-databind ~> 2.6.7.1.

Always verify the validity and compatibility of suggestions with your codebase.

Review vulnerable dependency
Automate Security Workflow

GitHub

Security Alerts

Depency Graph

Raw DB of GitHub Alerts with CVE info

POCs on GitHub Projects and Related Info

Slack

Email

JIRA Tickets

JIRA API

GraphQL API v4

Screwdriver Cron Job
If you are in the audience or you work for GitHub, help us automate OSPOs workflows.
We’d love your help

Project: https://github.com/yahoo/GitHub-Security-Alerts-Workflow

- Add automation for different solutions
  - JIRA
  - Email
  - Slack
- Contribute GitHub security alerts to GHcrawler
Open Source has more potential to be secure
But that’s only if you take advantage of the information available in the open source community and patch vulnerable dependencies.

And contribute back.
Thank You

- Gil Yehuda, Verizon Media
- Justin Hutchings, GitHub
- Jamie Jones, GitHub
- Jeff McAffer, Microsoft
- James Siri, Amazon
- Manikandan Subramaniam, Verizon Media
- Henri Yandell, Amazon
- Simon Maple, Snyk
Thank You

Ashley Wolf
Open Source Program Manager
Verizon Media
awolf@verizonmedia.com

Twitter: @Meta_Ashley
References

- https://github.com/jamesiri/github-cve-report-poc
- https://github.blog/2017-11-16-introducing-security-alerts-on-github/
- https://github.com/microsoft/ghcrawler
- https://www.emojione.com/emoji/v