

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!
DEVELOPER NETWORK

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

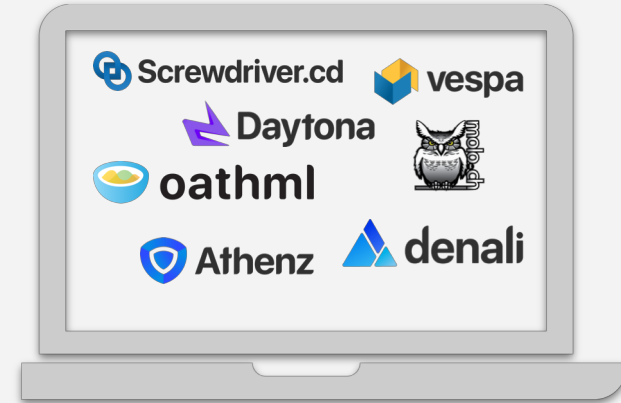
Active Open Source Projects published by Verizon Media


25

GitHub organizations that we manage

200+

Mobile and TV Applications that rely upon our services for compliance



 Yahoo Open Source

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.

The screenshot shows the Verizon Media Bug Bounty Program page on the HackerOne platform. The page features a red header with the Verizon Media logo and navigation links. Below the header, there is a navigation bar with links for Policy, Hactivity, Thanks, and Updates (4). A green 'Submit Report' button is also visible. The main content area is divided into two columns. The left column contains the 'Policy' section, which includes a 'Welcome to Verizon Media' message and a 'We are Paranoid' section. The right column contains a 'Response Efficiency' section with statistics and a 'Program Statistics' section with bounty details.

hackerone FOR BUSINESS FOR HACKERS HACKTIVITY COMPANY TRY HACKERONE

Verizon Media
Build Brands Members Love
Bug Bounty Program
www.verizonmedia.com · @verizonmedia · Launched on February 3rd, 2014

Policy Hactivity Thanks Updates (4) Submit Report


Policy

Welcome to Verizon Media

With brands like Yahoo, HuffPost and TechCrunch, Verizon Media helps people stay informed and entertained, communicate and transact, while creating new ways for advertisers and partners to connect. With technologies like XR, AI, machine-learning, and 5G, we're transforming media for tomorrow, too.

We are Paranoid

Our information security team is known as the Paranoids, and we're committed to protecting our brands and our users. As part of this commitment, we invite security researchers to help protect Verizon Media and its users by proactively identifying security vulnerabilities via our bug bounty program. Our program is inclusive of all Verizon Media brands and offers competitive rewards for a wide array of vulnerabilities. We encourage security researchers looking to participate in our bug bounty program to review our policy to ensure compliance with our rules and also to help you safely verify any vulnerabilities you may uncover.



Paranoids

Response Efficiency

7 hrs
Average time to first response

2 days
Average time to triage

25 days
Average time to bounty

99% of reports
Meet response standards
Based on last 90 days

Program Statistics

\$50
Minimum bounty

> \$4,000,000
Total bounties paid

\$300 - \$460

verizon

**We're talking about vulnerabilities
that are in a published piece of code.**



OSPPOs 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

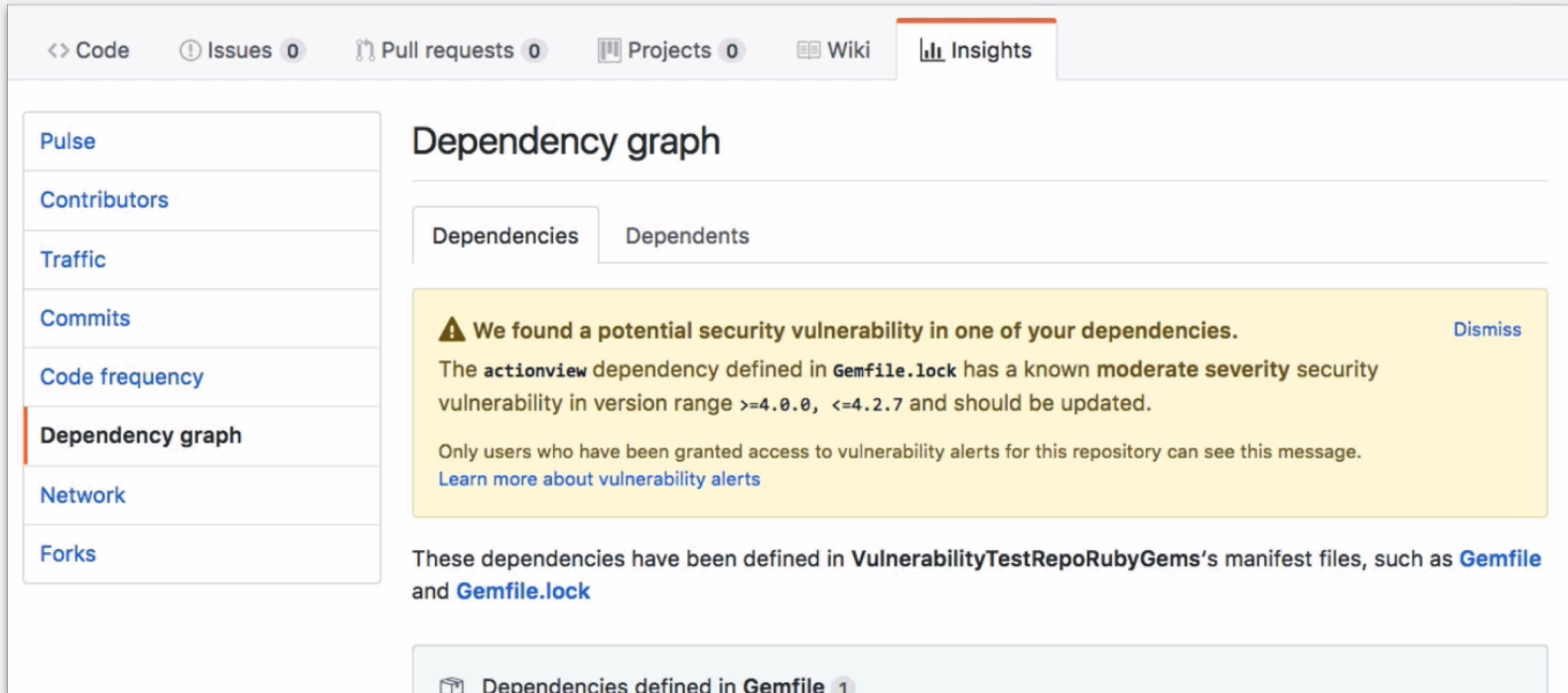
- What GitHub does to help your companies' open source security issues
- Where the alerts and APIs fall short
- A call for you to help develop a better solution

GitHub Provides Security Alerts

The screenshot shows the GitHub repository page for 'yahoo/mendel'. At the top, there are navigation links for 'Code', 'Issues 19', 'Pull requests 0', 'Projects 2', 'Wiki', 'Insights', and 'Settings'. Below these are repository statistics: '736 commits', '8 branches', '105 releases', '12 contributors', and 'MIT' license. A prominent yellow banner with a warning icon states: 'We found potential security vulnerabilities in your dependencies. You can see this message because you have been granted access to vulnerability alerts for this repository. Manage your notification settings or learn more about vulnerability alerts.' A 'See security alerts' button is located to the right of the banner. Below the banner, there are buttons for 'Branch: master', 'New pull request', 'Create new file', 'Upload files', 'Find file', and 'Clone or download'. The file list below shows various files and folders with their commit messages and dates.

File/Folder	Commit Message	Time
docs	Mdown to md for congruency	2 years ago
examples	full-example package-lock without mendel deps	a year ago
packages	Publish	3 months ago
test	Bring back postProcessManifest from accidental deletion	2 years ago
.agignore	agignore to help silver-searcher users	3 years ago
.editorconfig	Getting SSR to work	2 years ago
.eslintignore	eslint on npm test	3 years ago
.eslintrc	Suggest single quote for better consistency	2 years ago
.gitignore	Tests passing again; browserify interface works again; eslint pass again	2 years ago
.npmignore	Package upgrades for release	2 years ago
.prettiignore	Add prettierignore	a year ago
.prettierrc	Prettier config	a year ago
LICENSE	Initial commit	3 years ago

GitHub Security Alerts

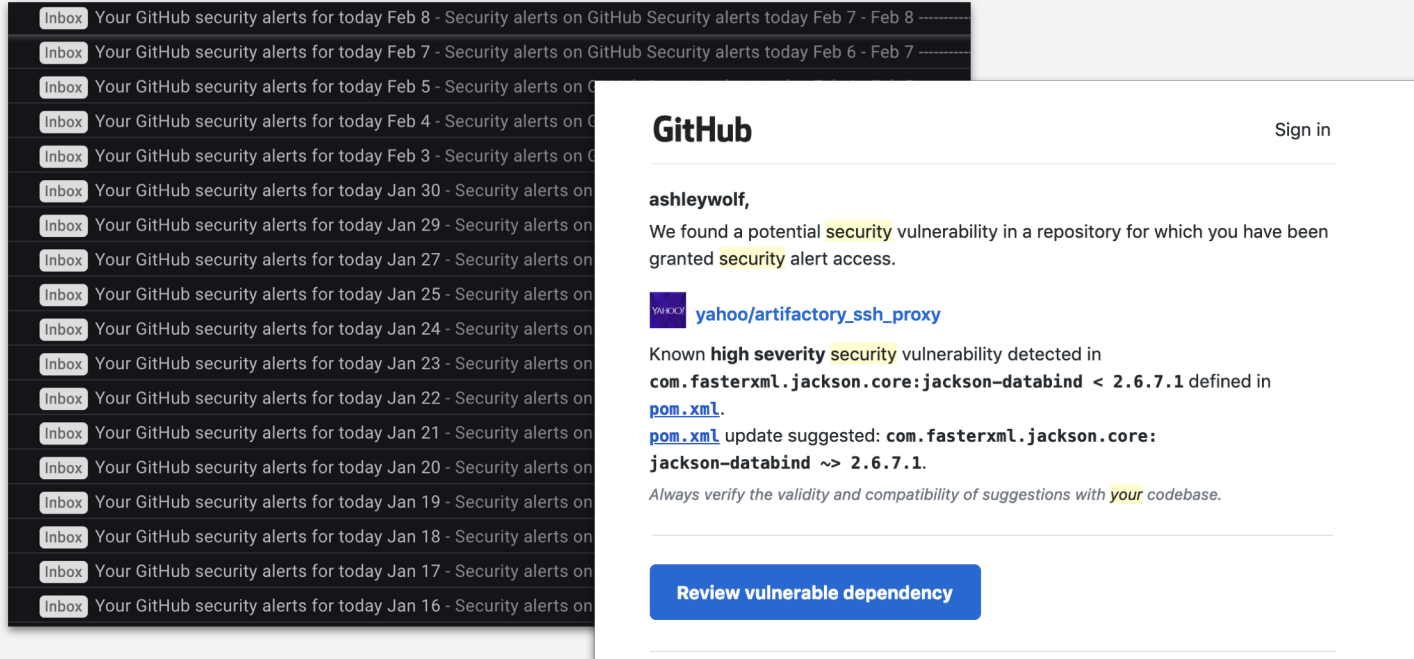


The screenshot shows the GitHub Insights interface for a repository. The top navigation bar includes links for Code, Issues (0), Pull requests (0), Projects (0), Wiki, and Insights. The left sidebar contains navigation options: Pulse, Contributors, Traffic, Commits, Code frequency, Dependency graph (selected), Network, and Forks. The main content area is titled "Dependency graph" and has two tabs: "Dependencies" (selected) and "Dependents". A prominent yellow alert box contains the following text: "⚠️ We found a potential security vulnerability in one of your dependencies. Dismiss". Below this, it states: "The `actionview` dependency defined in `Gemfile.lock` has a known moderate severity security vulnerability in version range `>=4.0.0, <4.2.7` and should be updated." It also notes: "Only users who have been granted access to vulnerability alerts for this repository can see this message." and provides a link: "Learn more about vulnerability alerts". Below the alert, it says: "These dependencies have been defined in `VulnerabilityTestRepoRubyGems`'s manifest files, such as `Gemfile` and `Gemfile.lock`". At the bottom, a section header reads: "Dependencies defined in `Gemfile` 1".

The vast majority (81%) of vulnerable dependencies may be fixed by simply updating to a new version

<https://arxiv.org/abs/1808.09753>

GitHub Email Alerts




The image shows a screenshot of an email inbox on the left, with a detailed view of a GitHub security alert email on the right. The email is from GitHub to 'ashleywolf' and informs them of a potential security vulnerability in a repository they have access to. The vulnerability is in the 'com.fasterxml.jackson.core:jackson-databind' library, version 2.6.7.1, which is defined in a 'pom.xml' file. The email suggests updating to version 2.6.7.1 and includes a button to 'Review vulnerable dependency'. The email also includes a 'Sign in' link in the top right corner.

GitHub Sign in

ashleywolf,

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

 [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

yahoo / mendel

Watch 14 Star 85 Fork 24

Code Issues 19 Pull requests 0 Projects 2 Wiki Insights Settings

Pulse
Contributors
Community
Traffic
Commits
Code frequency
Dependency graph
Alerts
Network
Forks

People

Alerts

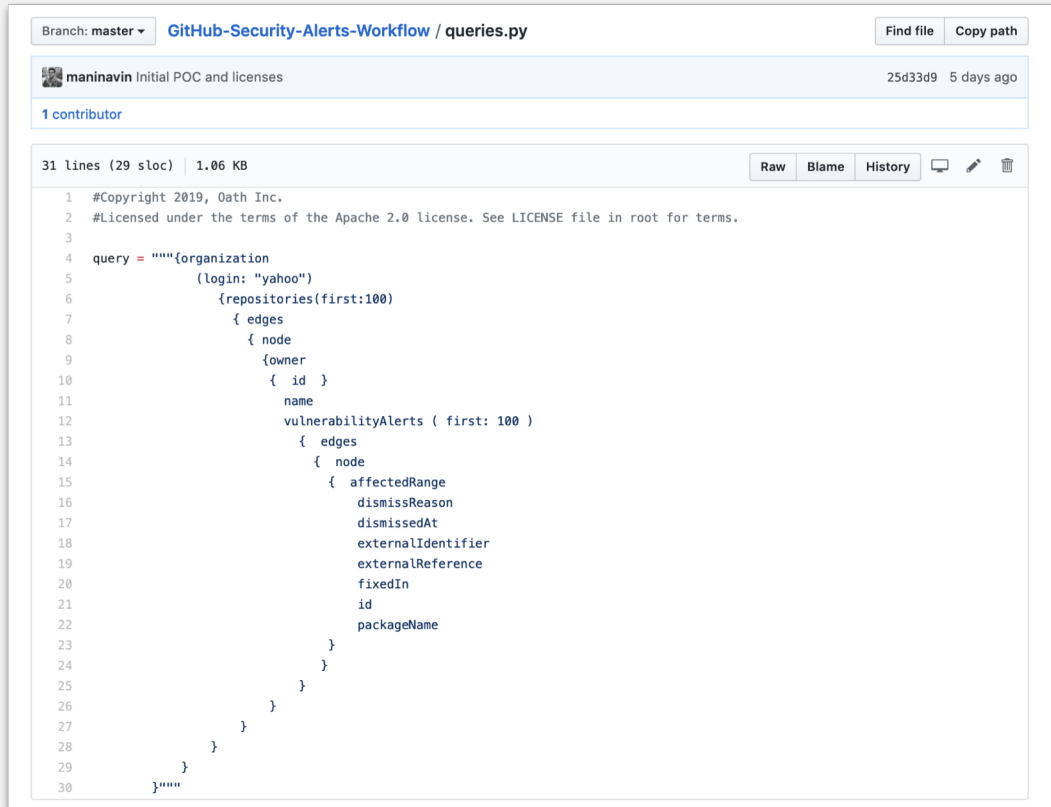
Dismiss all

▲ 25 Open ✓ 3 Closed Sort

▲ deep-extend	opened on Oct 8, 2018 by GitHub • examples/full-example/package-lock.json	high severity
▲ cryptiles	opened on Dec 13, 2018 by GitHub • packages/karma-mendel/package-lock.json	high severity
▲ deep-extend	opened on Dec 13, 2018 by GitHub • examples/planout-example/package-lock.json	high severity
▲ cryptiles	opened on Dec 13, 2018 by GitHub • packages/mendel-deps/package-lock.json	high severity
▲ cryptiles	opened on Dec 13, 2018 by GitHub • examples/full-example/package-lock.json	high severity
▲ mixin-deep	opened on Dec 13, 2018 by GitHub • examples/planout-example/package-lock.json	high severity
▲ cryptiles	opened on Dec 13, 2018 by GitHub • package-lock.json	high severity
▲ sshpk	opened on Dec 13, 2018 by GitHub • packages/karma-mendel/package-lock.json	moderate severity
▲ hoek	opened on Dec 13, 2018 by GitHub • packages/mendel-deps/package-lock.json	moderate severity
▲ atob	opened on Oct 8, 2018 by GitHub • examples/full-example/package-lock.json	moderate severity
▲ cached-path-relative	opened on Dec 13, 2018 by GitHub • examples/planout-example/package-lock.json	moderate severity
▲ hoek	opened on Dec 13, 2018 by GitHub • package-lock.json	moderate severity
▲ atob	opened on Dec 13, 2018 by GitHub • packages/mendel-deps/package-lock.json	moderate severity
▲ sshpk	opened on Dec 13, 2018 by GitHub • packages/mendel-deps/package-lock.json	moderate severity

Automating Security Workflow Project

Automate Security Workflow



Branch: master | GitHub-Security-Alerts-Workflow / queries.py

maninavin Initial POC and licenses 25d33d9 5 days ago

1 contributor

31 lines (29 sloc) | 1.06 KB

```
1 #Copyright 2019, Oath Inc.
2 #Licensed under the terms of the Apache 2.0 license. See LICENSE file in root for terms.
3
4 query = """{organization
5     (login: "yahoo")
6     {repositories(first:100)
7       {edges
8         {node
9           {owner
10            { id }
11            name
12            vulnerabilityAlerts ( first: 100 )
13              { edges
14                { node
15                  { affectedRange
16                    dismissReason
17                    dismissedAt
18                    externalIdentifier
19                    externalReference
20                    fixedIn
21                    id
22                    packageName
23                  }
24                }
25              }
26            }
27          }
28        }
29      }
30    }"""
```

Automating the Alert Workflow




GitHub

Sign in

ashleywolf,

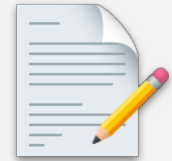
We found a potential security vulnerability in a repository for which you have been granted security alert access.

 [yahoo/artifactory_ssh_proxy](#)

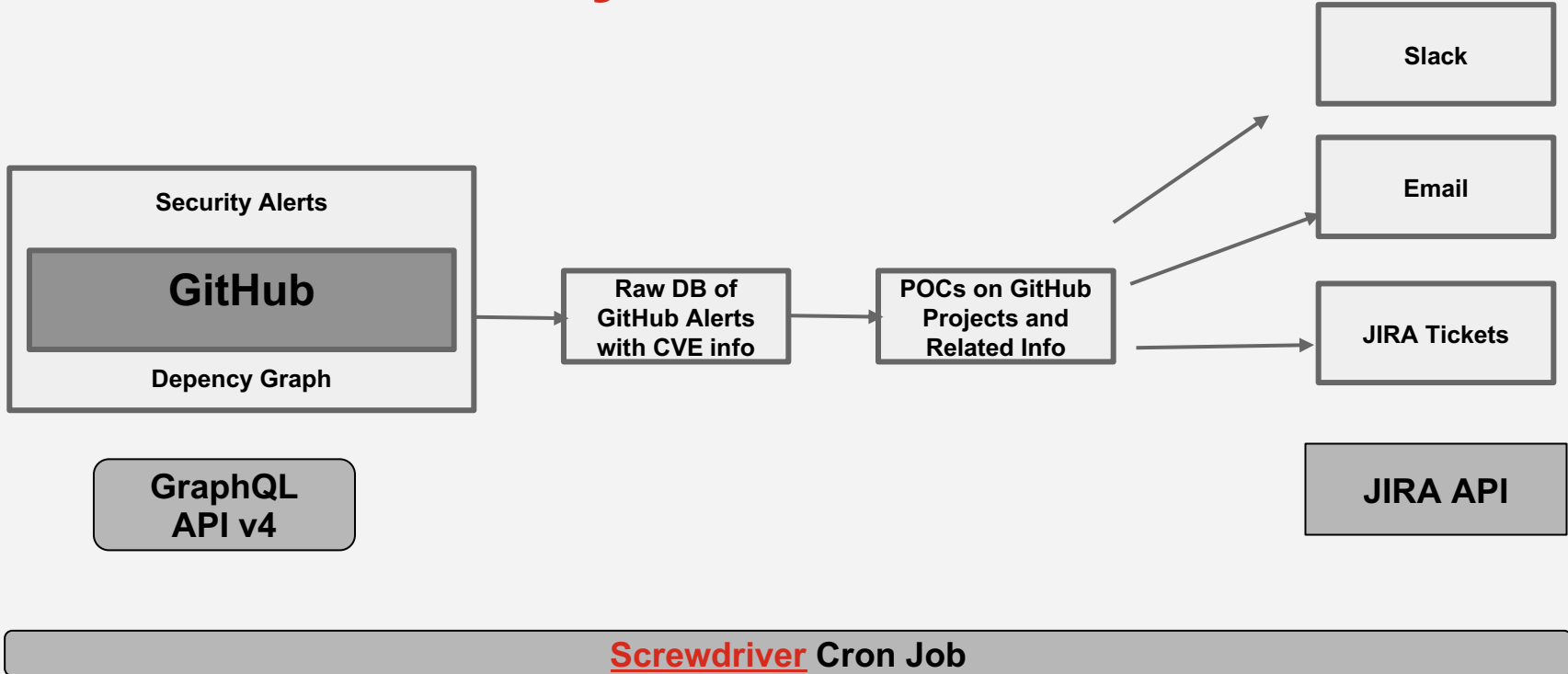
Known high severity security vulnerability detected in `com.fasterxml.jackson.core:jackson-databind < 2.6.7.1` defined in [pom.xml](#).
[pom.xml](#) update suggested: `com.fasterxml.jackson.core:jackson-databind ~> 2.6.7.1`.

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

[Review vulnerable dependency](#)



Automate Security Workflow



Security Advisory Event

```
{
  "action": "published",
  "security_advisory": {
    "ghsa_id": "GHSA-rf4j-j272-fj86",
    "summary": "Moderate severity vulnerability that affects django",
    "description": "django.contrib.auth.forms.AuthenticationForm in Django 2.0 before 2",
    "severity": "moderate",
    "identifiers": [
      {
        "value": "GHSA-rf4j-j272-fj86",
        "type": "GHSA"
      },
      {
        "value": "CVE-2018-6188",
        "type": "CVE"
      }
    ],
    "references": [
      {
        "url": "https://nvd.nist.gov/vuln/detail/CVE-2018-6188"
      }
    ],
    "published_at": "2018-10-03T21:13:54Z",
    "updated_at": "2018-10-03T21:13:54Z",
    "withdrawn_at": null,
    "vulnerabilities": [
      {
        "package": {
          "ecosystem": "pip",
          "name": "django"
        },
        "severity": "moderate",
        "vulnerable_version_range": ">= 2.0.0, < 2.0.2",
        "first_patched_version": {
          "identifier": "2.0.2"
        }
      },
      {
        "package": {
          "ecosystem": "pip",
          "name": "django"
        },
        "severity": "moderate",
        "vulnerable_version_range": ">= 1.11.8, < 1.11.10",
        "first_patched_version": {
          "identifier": "1.11.10"
        }
      }
    ]
  }
}
```

Repository Vulnerability Alert Event

```
{
  "action": "dismiss",
  "alert": {
    "id": 7649605,
    "affected_range": "0.2.0",
    "affected_package_name": "many_versioned_gem",
    "external_reference": "https://nvd.nist.gov/vuln/detail/CVE-2018-3728",
    "external_identifier": "CVE-2018-3728",
    "fixed_in": "0.2.5",
    "dismitter": {
      "login": "octocat",
      "id": 1,
      "node_id": "MDQ6VXNlcjIxMDMxMDY3",
      "avatar_url": "https://github.com/images/error/octocat_happy.gif",
      "gravatar_id": "",
      "url": "https://api.github.com/users/octocat",
      "html_url": "https://github.com/octocat",
      "followers_url": "https://api.github.com/users/octocat/followers",
      "following_url": "https://api.github.com/users/octocat/following{/other_user}",
      "gists_url": "https://api.github.com/users/octocat/gists{/gist_id}",
      "starred_url": "https://api.github.com/users/octocat/starred{/owner}/{repo}",
      "subscriptions_url": "https://api.github.com/users/octocat/subscriptions",
      "organizations_url": "https://api.github.com/users/octocat/orgs",
      "repos_url": "https://api.github.com/users/octocat/repos",
      "events_url": "https://api.github.com/users/octocat/events{/privacy}",
      "received_events_url": "https://api.github.com/users/octocat/received_events",
      "type": "User",
      "site_admin": true
    },
    "dismiss_reason": "No bandwidth to fix this",
    "dismissed_at": "2017-10-25T00:00:00+00:00"
  }
}
```

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://help.github.com/en/articles/about-security-alerts-for-vulnerable-dependencies>
- <https://arxiv.org/abs/1808.09753>
- <https://github.com/microsoft/ghcrawler>
- <https://www.oreilly.com/library/view/securing-open-source/9781491996980/ch01.html>
- <https://www.emojione.com/emoji/v>