

GitHub Security Alerts

An Executive Summary

Gavin H. Smith

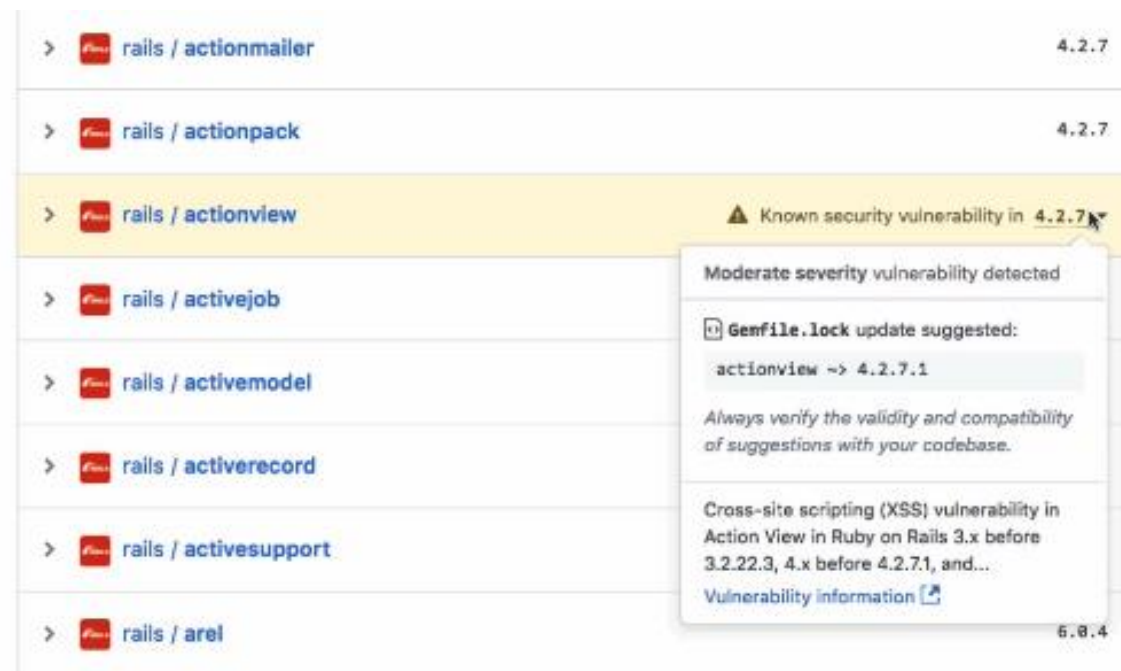


What are GitHub Security Alerts?

- Tracks vulnerable dependencies that your repository uses
- Supports Java, Ruby, Python, .NET, JavaScript dependencies

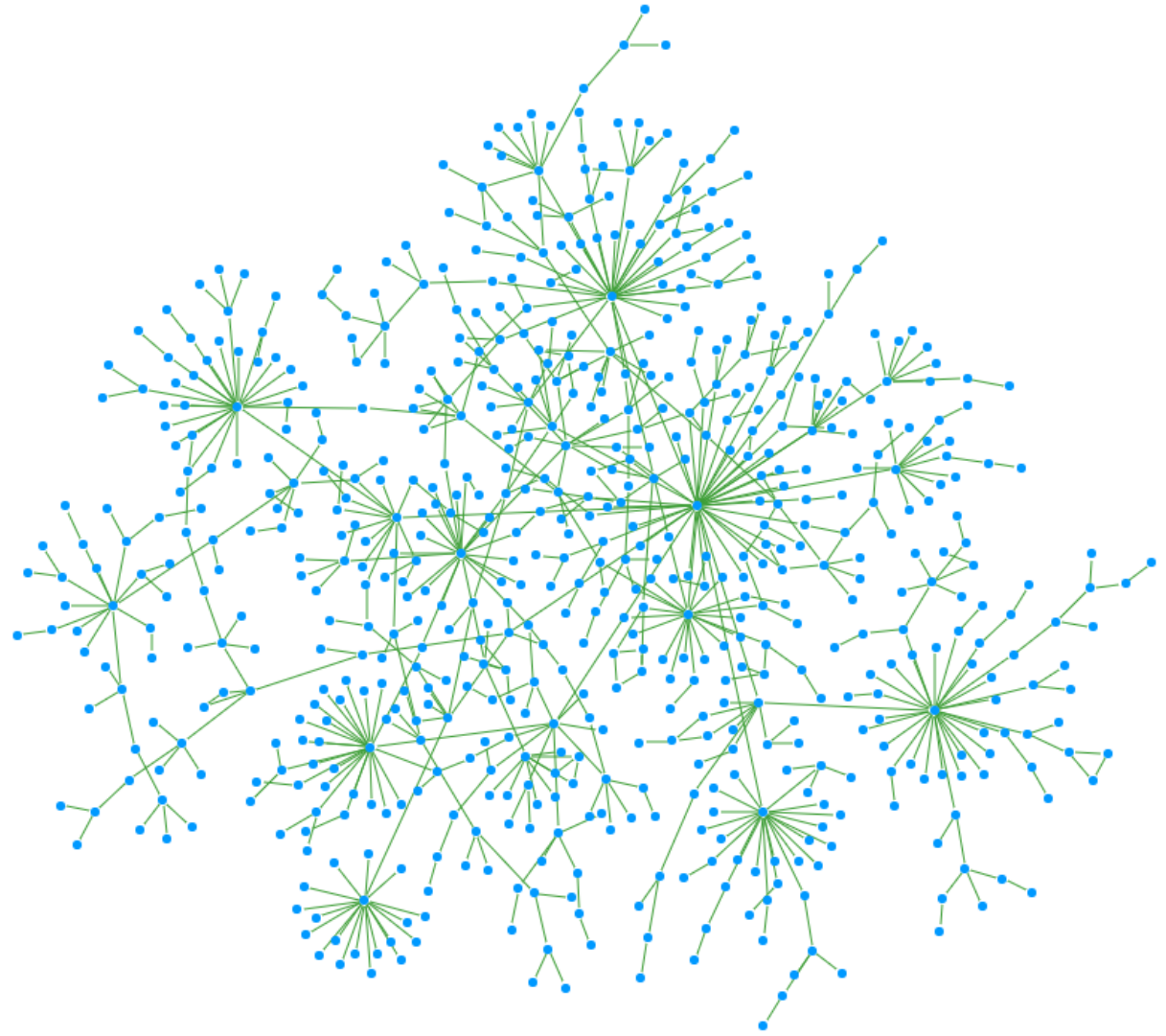
How GitHub security alerts work

- Under the insights tab on your GitHub repository is listed “Alerts”
- Lists dependencies that are vulnerable
 - Contains the level of severity of the vulnerability in the dependency as well as the CVE id



Dependencies

- When one package or piece of software depends on other packages or software.
- Vulnerabilities in dependencies can lead to vulnerabilities in your software.



CVE (Common Vulnerabilities and Exposures)

- Operated and maintained by the MITRE corporation.
- Lists information known about publicly known about certain security vulnerabilities.
- Each instance is a specific vulnerability in a software.

CVE-2014-0160 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

Source: MITRE

Description Last Modified: 04/07/2014

[+View Analysis Description](#)

Impact

CVSS v2.0 Severity and Metrics:

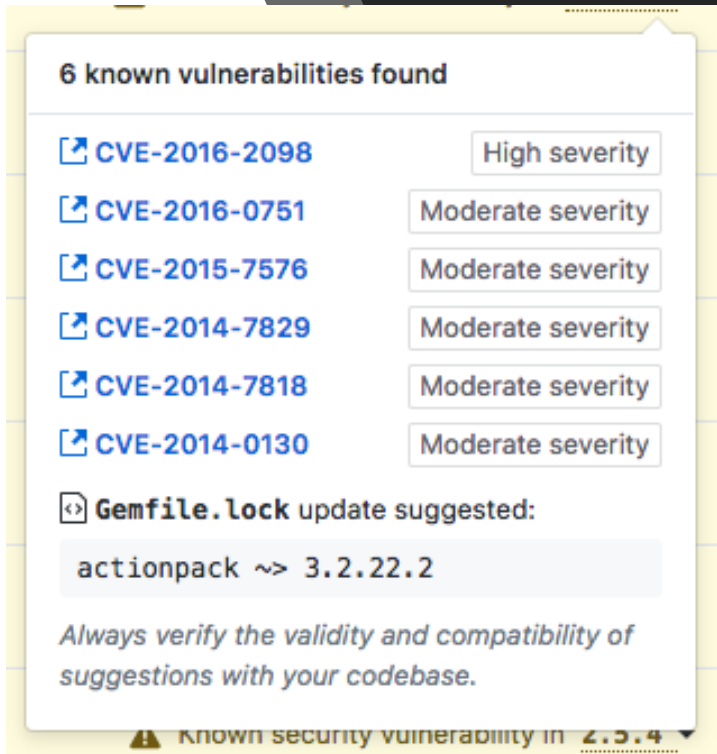
Base Score: 5.0 MEDIUM

Vector: (AV:N/AC:L/Au:N/C:P/I:N/A:N) (V2 legend)

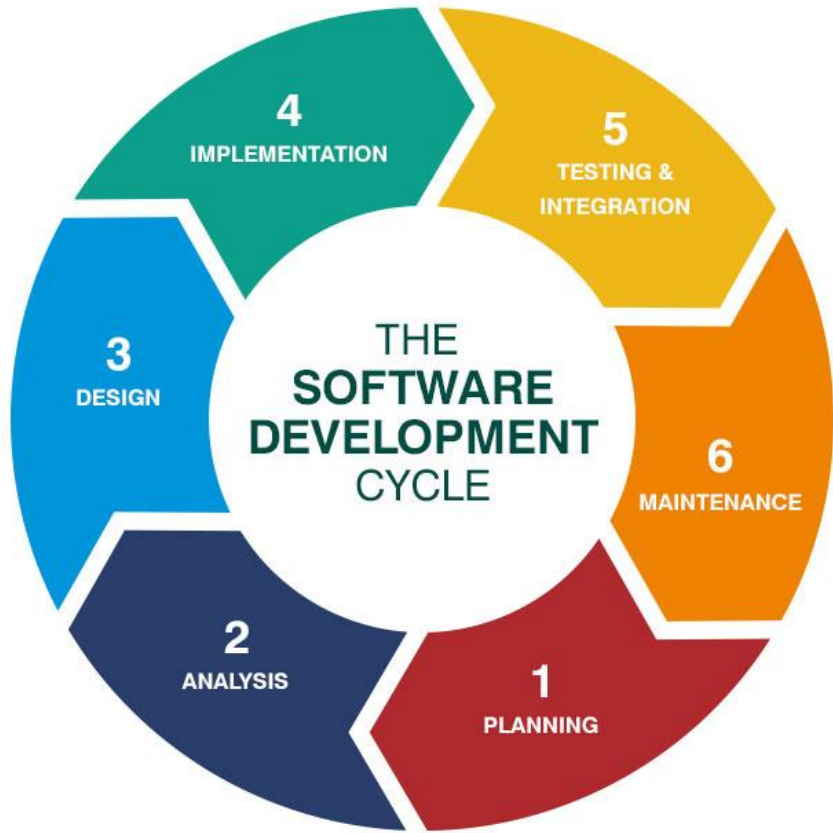
Impact Subscore: 2.9

Exploitability Subscore: 10.0

How you can utilize GitHub alerts



- Read the CVE and understand the vulnerability associated with the dependency.
- Check to see how the vulnerability is used in your project.
- Check what the updated version of the software is and that it is compatible with your project.
- Update the software and test your project for functionality, then merge the update.



Working with GitHub Alerts

- GitHub alerts do not have to be a feature that is only helpful after a product is pushed to production. GitHub alerts start immediately after pushing code to its repository, so developers can fix bugs and vulnerabilities before they become impractical to fix.

Benefits



Gives an easier pathway to resolving vulnerabilities in your repositories' code



Gives your developers a deeper understanding of the security issues involved with the software your project uses



Protects the users' information and data



Establishes a framework for your company to deal with future issues that require updating your systems.

Example of not properly updating code

- In the summer of 2017 Equifax, one of the largest credit agencies in the United States, was hacked because they did not update a vulnerable Java framework, Apache Struts, on all of their systems.
- Lead to over 148 million people having their private information stolen
- Found by the US House Oversight and Government Reform committee to be due to negligence.

Could GitHub Security Alerts Have Helped?

- Although in cases like this, it is not certain that GitHub Security Alerts could have directly helped, it still shows how large hacks of this nature are due to just simply not updating code.
- GitHub Security Alerts would have made it more clear to the developers exactly which products that the company controls contain the vulnerable software (as many other products that contained the vulnerable software were fixed in time).



The Equifax Data Breach

Majority Staff Report
115th Congress
December 2018


Equifax breach was 'entirely preventable' had it used basic security measures, says House report

Why Should You Use This?

- Avoid public scrutiny
- Not taking proper measures can be illegal
- Investing in security looks good to users and the public



But really, why?

- Computer and cyber security is in everyone's best interest, to not invest in it for the future would be unethical. Companies that have sensitive information of their users (like Equifax) have an even higher responsibility to be as scrupulous as possible over their security measures.
 - Companies like GitHub are making it easier and easier for developers to work security into their workflow.
- 

What not to do

Ignore the alerts

It's easy to ignore them when there are so many, can seem unimportant

Improvements
going forward

For GitHub

- Create a way that these alerts can be more actionable, leaving the bulk of the work for the developers can lead to complacency

Improvements
going forward

For Developers/Organizations

- Install a system for updating and maintaining software security
- Teach IT/engineers to read all alerts and warnings.

Improvements
going forward

For governmental regulatory bodies

- Punish companies who knowingly choose to engage in negligent practices that lead to the exposure of sensitive information. If companies are not held responsible they have no incentive in the future to invest in proper computer security.

In Summary

- Take advantage of any help that companies give you in securing your products.
 - Including things like GitHub Alerts as well as free databases like MITRE's CVE.
- GitHub Security Alerts are a step in the right direction.
- Fixing code does not have to require large and costly system wide updates, can be worked into development cycle.
- Companies, developers, anyone who codes, and lawmakers should all participate in good security practices.

Resources

account, GitHubVerified. “GitHub (@Github).” *Twitter*, Twitter, 11 Dec. 2018, twitter.com/github.

“Committee Releases Report Revealing New Information on Equifax Data Breach.” *United States House Committee on Oversight and Government Reform*, 10 Dec. 2018, oversight.house.gov/report/committee-releases-report-revealing-new-information-on-equifax-data-breach/.

Ghoshal, Abhimanyu. “GitHub Will Now Alert You of Security Flaws in Your Project Dependencies.” *The Next Web*, 17 Nov. 2017, thenextweb.com/apps/2017/11/17/github-will-now-alert-you-of-security-flaws-in-your-project-depedencies/.

“Understanding the Dependency Concept.” *Understanding and Administering Systemd :: Fedora Docs Site*, docs.fedoraproject.org/ro/Fedora_Draft_Documentation/0.1/html/RPM_Guide/ch-dependencies.html.

“Committee Releases Report Revealing New Information on Equifax Data Breach.” *United States House Committee on Oversight and Government Reform*, 10 Dec. 2018, oversight.house.gov/report/committee-releases-report-revealing-new-information-on-equifax-data-breach/.