Open Source Vulnerability Notification

Brandon Carlson, Kevin Leach, Darko Marinov, Meiyappan Nagappan, and Atul Prakash

OSS 2019
Montreal, Canada
May 27, 2019

FA8750-15-2-0075
CNS-1646305
CNS-1646392
CNS-1740897
CNS-1740916

About the Authors

Brandon Carlson

- Recent Masters Graduate at UIUC
- 15 years in the software industry
- A Software Developer recently turned Data Scientist

Dr. Kevin Leach

- Senior Research Fellow at the University of Michigan

Dr. Darko Marinov

- Professor at the University of Illinois at Urbana-Champaign

Dr. Meiyappan (Mei) Nagappan

- Assistant Professor at the University of Waterloo

Dr. Atul Prakash

- Professor at the University of Michigan

Data Breaches the New Normal?

- High Profile Data Breaches Related to Vulnerable Dependencies
- OWASP Top 10
  - ○ Using Components With Known Vulnerabilities

EQUIFAX
PANAMA PAPERS
The secrets of dirty money
verticalscope
EXACTIS
MARRIOTT
BONVOY
AADHAAR

64% of the Open Source Projects Examined Contained at Least One Vulnerable Dependency

Only 19 Projects Contained a Vulnerability Notification Process

Open Source Project Dependencies

- How prevalent are vulnerable dependencies among projects?
- How common are security notification policies in open source projects?
- How available is contact information for open source projects?

Selected Open Source Projects

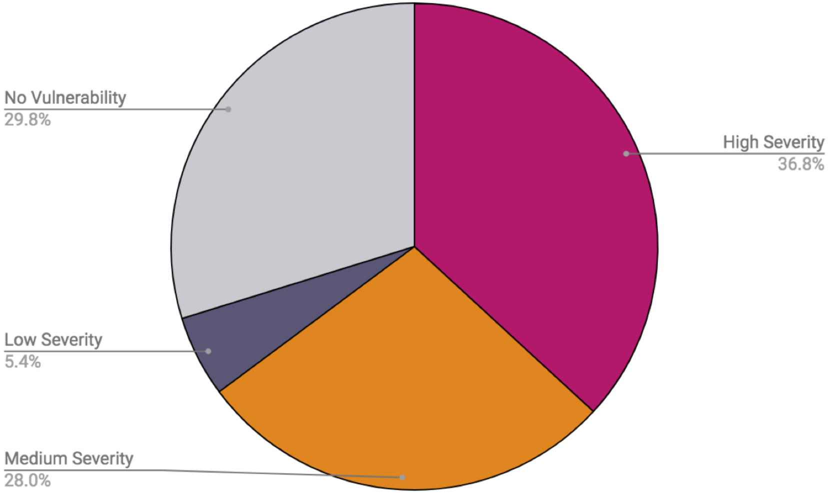
- 600 Java Projects Hosted on GitHub
  - Trending Projects
  - Government Sponsored
  - National Laboratories
  - Civic Hackers
  - Many more…
- Security Scanning Tools
  - Snyk
  - Custom Built Tool

How prevalent are vulnerable dependencies among the 600 projects?

385 Projects with Vulnerable Dependencies

- High Level Severity - 266
- Medium Level Severity - 202
- Low Severity - 39

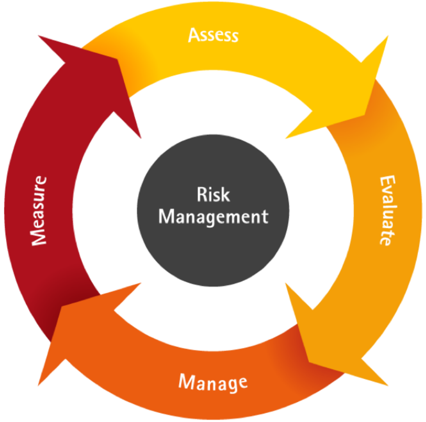
215 Projects No Known Vulnerability



64% Projects Scanned Contained a Vulnerable Dependency

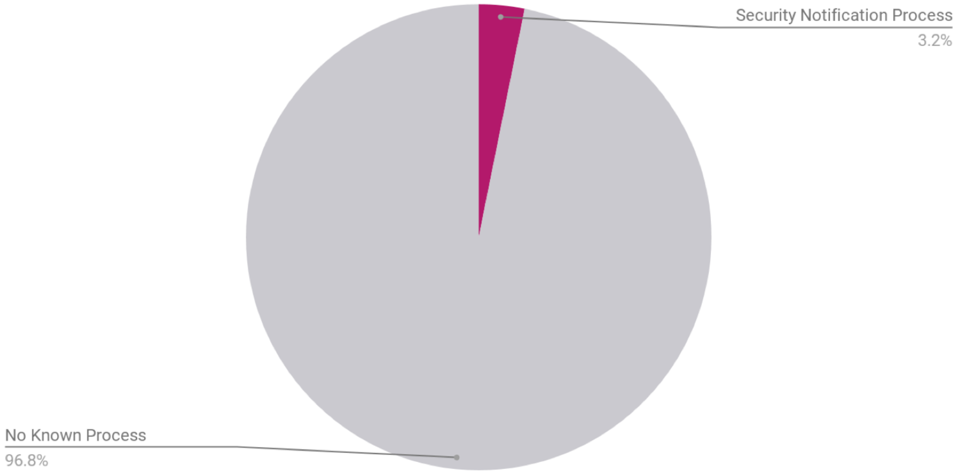
Risk of Using Vulnerable Dependencies

- Using a vulnerable dependency **does not** guarantee the open source project can easily be exploited
- It **does** represent a risk to the open source project
- Vulnerable dependencies **should** be updated based on
  - Level of Acceptable Risk Posed
  - Severity of the Issue
  - As Part of the Development Cycle



How common are security notification policies in open source projects?

- 385 Open Source Projects Contain a Vulnerable Dependency
  - 13 Security Reporting Process
  - 372 No Reporting Process Found
- Of the 600 Open Source Projects
  - 19 Security Reporting Process
  - 581 No Reporting Process Found

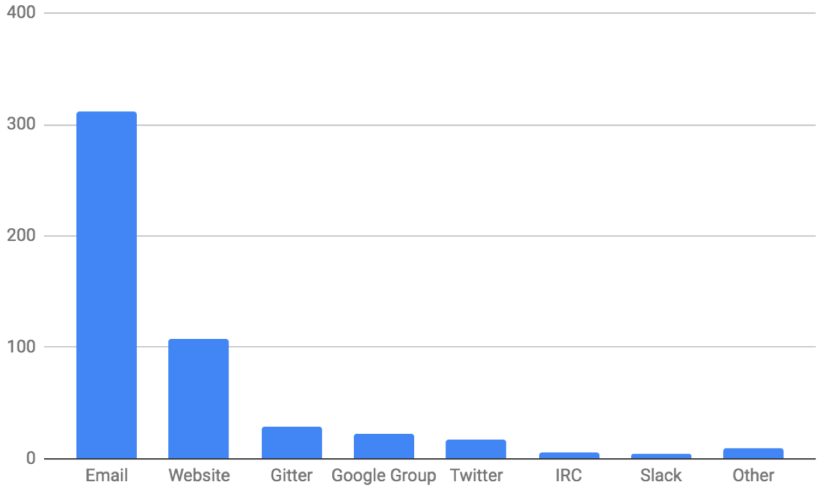


Security Reporting Processes at Scale

- Using Repository Dumps from:
  - GitHub
  - GitLab
  - BitBucket
- Over 30 Million Repos
- Curated Lists of BugCrowd and HackerOne
- Scanned using both the Project Owner’s Name and Project Name
- Only 6,645 Open Source Projects had a bug bounty program

How available is contact information for open source projects?

- Only 119 of 600 Open Source Projects Contained No Contact Information
- Remaining 481 had Publicly Available Contact Information
- ~44 seconds on average to find the contact information per project

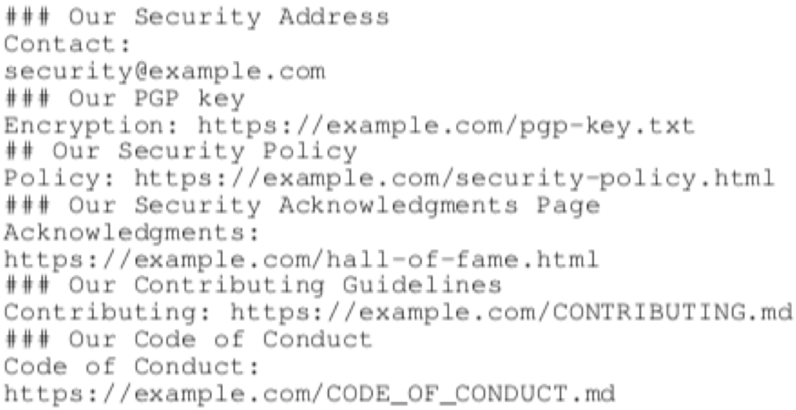


Recommendations

- Community Driven Improvements
- Open Source Repository Changes

SECURITY.md Mechanism for Vulnerability Notification

- Similar to the Security.txt Initiative
- Snyk Provides a Similar Recommendation
- Standardize the Open Source Security Disclosure Process
- Addresses an Issue Found in a 2017 GitHub Open Source Survey
- Ability to Affect Change Today



```
### Our Security Address
Contact:
security@example.com
### Our PGP key
Encryption: https://example.com/pgp-key.txt
## Our Security Policy
Policy: https://example.com/security-policy.html
### Our Security Acknowledgments Page
Acknowledgments:
https://example.com/hall-of-fame.html
### Our Contributing Guidelines
Contributing: https://example.com/CONTRIBUTING.md
### Our Code of Conduct
Code of Conduct:
https://example.com/CODE_OF_CONDUCT.md
```

Adapting Hosts to Facilitate Security Disclosures

- Verified Researcher Tags
- Private Pull Requests & Issues
- On Creation of a Repository, Allow for Adding the Security.md

SECURITY.md

What's Next?

- Further Inform Open Source Community of the Usage of Vulnerable Dependencies
- Push for Standardization of the Security Reporting Process
- Encourage Repository Providers to Continue to Evolve their Security Notification Processes

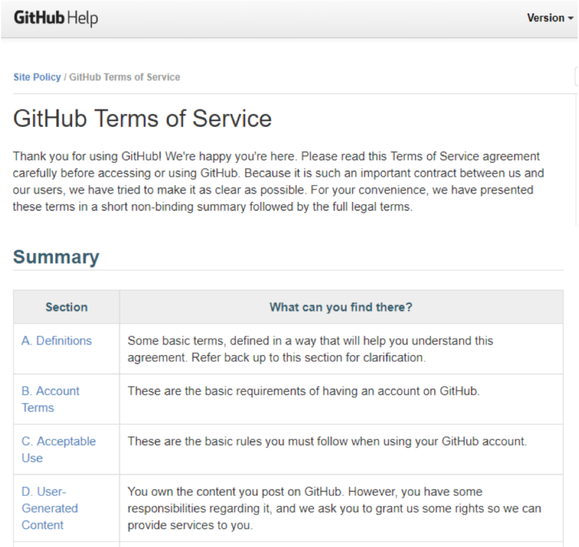
- Thank You Snyk!

Contact: blcarlson@gmail.com

Backup Slides

Open Source Project Owners' Response?

- Attempted to Understand Open Source Project Owners' Response
  - Pull Requests with Verified Updated Dependencies
  - Opening Issues to Inform Project Owner
- Result from ~30 PR or Issues Created
  - Responses Varied
- GitHub Account Suspended
  - Violation of Terms of Service



GitHub Terms of Service

Thank you for using GitHub! We're happy you're here. Please read this Terms of Service agreement carefully before accessing or using GitHub. Because it is such an important contract between us and our users, we have tried to make it as clear as possible. For your convenience, we have presented these terms in a short non-binding summary followed by the full legal terms.

Summary

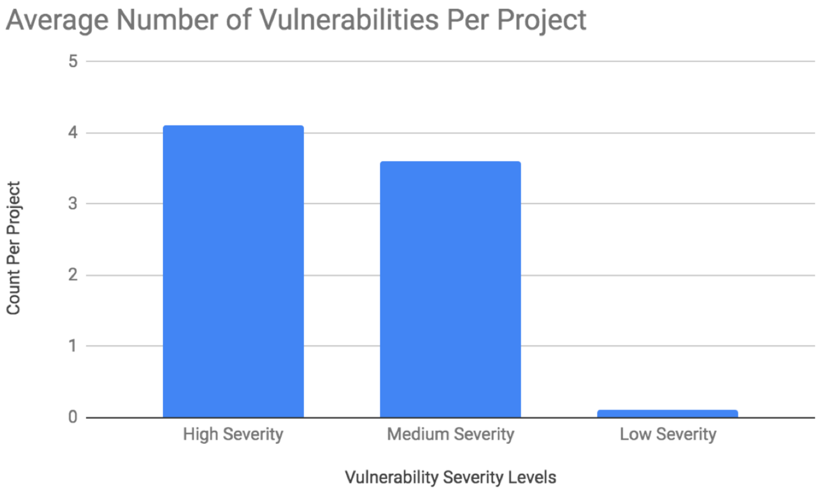
Section	What can you find there?
A. Definitions	Some basic terms, defined in a way that will help you understand this agreement. Refer back up to this section for clarification.
B. Account Terms	These are the basic requirements of having an account on GitHub.
C. Acceptable Use	These are the basic rules you must follow when using your GitHub account.
D. User-Generated Content	You own the content you post on GitHub. However, you have some responsibilities regarding it, and we ask you to grant us some rights so we can provide services to you.

How prevalent are vulnerable dependencies among the projects?

Average of 7.8 Vulnerable Dependencies Per Project (Includes Direct or Transitive)

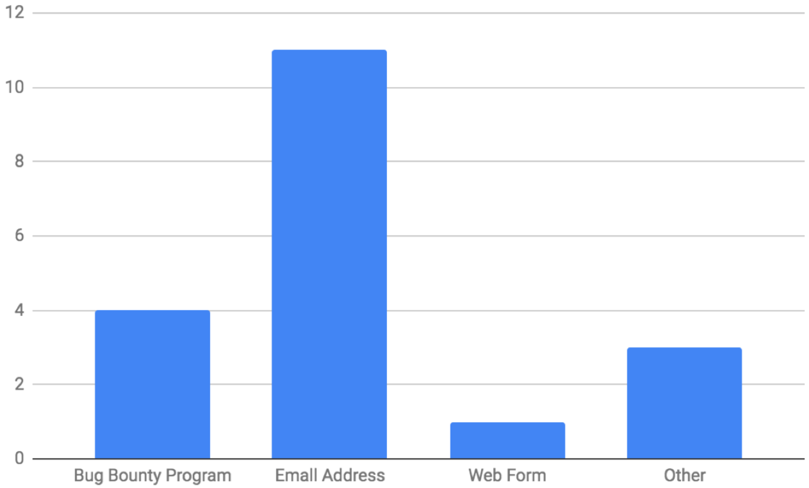
- High Severity - 4.1
- Medium Severity - 3.6
- Low Severity - 0.1

A number of projects scanned used dependencies that had hundreds of vulnerabilities.



Found Security Reporting Processes

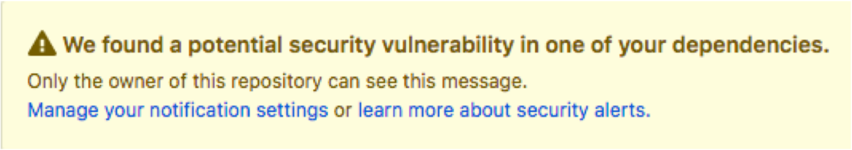
- 19 Found Security Reporting Policies
  - Bug Bounty Program
  - Email Address
  - Web Form
  - Other



Related Initiative

- Weekly Email from GitHub containing security alerts for the week
- Security Alerts on the homepage of the Open Source Project

GitHub security alert digest



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

Only the owner of this repository can see this message.

Manage your notification settings or learn more about security alerts.