Lessons from Covid-19
A Community-Based Approach to Securing Open Source Software
Pedro Nacht, Software Engineer  
Google Open Source Security Team  
LinkedIn: pedro-nacht

Nikita Jain, Product Marketing Manager  
Cybersecurity, Google  
LinkedIn: nikitajain88
Exponential growth of Covid

source: hindustantimes.com

source: nextstrain.com
Exponential growth of Covid
Exponential growth of Covid

software Supply chain attacks

Increase in software supply chain attacks, 2019-2023 (source: Sonatype [modified])

An open source project and its dependencies (source: deps.dev)
Exponential growth of Covid

Increase in software supply chain attacks, 2019-2023 (source: Sonatype [modified])

An open source project and its dependencies (source: deps.dev)
AGENDA

1. What is open source security?
2. What are supply chain attacks?
3. A side trip into your dependencies!
4. Lessons from Covid
5. Questions
AGENDA

1. What is open source security?
2. What are supply chain attacks?
3. A side trip into your dependencies!
4. Lessons from Covid
5. Questions
Open Source Software is everywhere
Including in **essential infrastructure**

- **Enterprise Software**: 96%
- **Healthcare**: 93%
- **Financial**: 97%
- **Energy Industry**: 100%

Percentage of surveyed codebases that contain open source code

*source: Synopsys*
ALL MODERN DIGITAL INFRASTRUCTURE

A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003
An overview of supply chain attacks...
Software supply chain attack: when a cyber threat actor infiltrates a software vendor's network and employs malicious code to compromise the software before the vendor sends it to their customers. The compromised software then compromises the customer's data or system. (cisa.gov)

i.e., injecting code into your project to harm those who depend on you
The Next Supply Chain Attack Vector: Open-Source Software
‘The Internet Is on Fire’

A vulnerability in the Log4j logging framework has security teams scrambling to put in a fix.

The Next Supply Chain Attack Vector: Open-Source Software
‘The Internet Is on Fire’
A vulnerability in the Log4j logging framework has security teams scrambling to put in a fix.

The Next Supply Chain Attack Vector: Open-Source Software

Rage-quit: Coder unpublished 17 lines of JavaScript and “broke the Internet”
‘The Internet Is on Fire’
A vulnerability in the Log4j logging framework has security teams scrambling to put in a fix.

The Next Supply Chain Attack Vector: Open-Source Software

Attacks on Software Supply Chains To Increase in Severity in 2023: Report

Rage-quit: Coder unpublished 17 lines of JavaScript and “broke the Internet”
‘The Internet Is on Fire’
A vulnerability in the Log4j logging framework has security teams scrambling to put in a fix.

The Next Supply Chain Attack Vector: Open-Source Software

Banking Sector Targeted in Open-Source Software Supply Chain Attacks

Attacks on Software Supply Chains To Increase in Severity in 2023: Report

Rage-quit: Coder unpublished 17 lines of JavaScript and “broke the Internet”
‘The Internet Is on Fire’
A vulnerability in the Log4j logging framework has security teams scrambling to put in a fix.

The Next Supply Chain Attack Vector: Open-Source Software

Software Supply Chain Attacks Hit 61% of Firms

Banking Sector Targeted in Open-Source Software Supply Chain Attacks

Attacks on Software Supply Chains To Increase in Severity in 2023: Report

Rage-quit: Coder unpublished 17 lines of JavaScript and “broke the Internet”
Researchers find 633% increase in cyber-attacks aimed at open source repositories

‘The Internet Is on Fire’
A vulnerability in the Log4j logging framework has security teams scrambling to put in a fix.

The Next Supply Chain Attack Vector: Open-Source Software

Software Supply Chain Attacks Hit 61% of Firms

Banking Sector Targeted in Open-Source Software Supply Chain Attacks

Attacks on Software Supply Chains To Increase in Severity in 2023: Report

Rage-quit: Coder unpublished 17 lines of JavaScript and “broke the Internet”
But the code is open to inspect!

So what’s the problem??
But the code is open to inspect!

So what’s the problem??
he emailed me and said he wanted to maintain the module, so I gave it to him. I don't get any thing from maintaining this module, and I don't even use it anymore, and haven't for years.
he emailed me and said he wanted to maintain the module, so I gave it to him. I don't get any thing from maintaining this module, and I don't even use it anymore, and haven't for years.
Open source security...

...and public health lessons??
Lessons Learned from the Lessons Learned in Public Health during the First Years of COVID-19 Pandemic

Alessia Marcassoli, Matilde Leonardi, Marco Passavanti, Valerio De Angelis, Enrico Bentivegna, Paolo Martelletti, and Alberto Raggi

Paul B. Tchounwou, Academic Editor
Three lessons to come!

1) Evaluating risks
2) Monitoring
3) Communication
A quick side trip...

into your dependencies

Thank you to Nicky Ringland (@nickyringland), Josie Anugerah, and Eve Martin-Jones of Google’s deps.dev team for sharing the following dependency diagrams and stats!
Dependencies
the projects you rely on

Dependents (or reverse dependencies)
the projects that rely on you
Idea!
Hack hack hack!

YOUR code
YOUR code

OTHER code

External contributor!
Add a dependency!
And another dependency!
Don’t forget THEIR dependencies!
Package it up…
And release to the world!

YOUR code

OTHER code

SHARING code
98% Of the time a package is affected by a vulnerability, it’s affected *indirectly*.

Computed by deps.dev: From all published libraries across npm, Go, Maven, PyPI, and Cargo
But it’s not actually this...
But it’s not actually this... It’s THIS.
But it’s not actually this... It’s THIS.
average number of *direct* dependencies for an npm package

6

Computed by deps.dev.
average number of *direct* dependencies for an npm package

6

average number of *indirect* dependencies for an npm package

110

Computed by deps.dev.
Direct dependencies
Indirect dependencies
Yikes!
Yikes!
Lesson 1
Knowledge is key: know the actual risk
Lesson 1
Knowledge is key: know the actual risk
Free tools!

- OpenSSF Scorecard — to understand a project’s risks
- Deps.dev website — to understand connections between projects
OpenSSF Scorecard Report

6.3

github.com/pnacht/cronk

COMM: 8b5162cc23dd5a2afa2501012ef61d2f59b7fa6
GENERATED AT: 2023-09-06

Dangerous-Workflow **CRITICAL**
Determines if the project’s GitHub Action workflows avoid dangerous patterns.

Branch-Protection **HIGH**
Determines if the default and release branches are protected with pull requests.

Code-Review **HIGH**
Determines if the project requires code review before pull requests.

Maintained **HIGH**
Determines if the project is “actively maintained”.

Binary-Artifacts **HIGH**
Determines if the project has generated executable (binary) artifacts in the source repository.

Dependency-Update-Tool **HIGH**
Determines if the project uses a dependency update tool.

Vulnerabilities **HIGH**
Determines if the project has open, known undefined vulnerabilities.

SAST **MEDIUM**
Determines if the project uses static code analysis tools.

8.1

github.com/tensorflow/tensorflow

COMM: 5d86fa87139fe1e5c2063ba93ac540c4f2baf
GENERATED AT: 2023-09-07

Dangerous-Workflow **CRITICAL**
Determines if the project’s GitHub Action workflows avoid dangerous patterns.

Token-Permissions **HIGH**
Determines if the project’s workflows follow the principle of least privilege.

Binary-Artifacts **HIGH**
Determines if the project has generated executable (binary) artifacts in the source repository.

Dependency-Update-Tool **HIGH**
Determines if the project uses a dependency update tool.

Maintained **HIGH**
Determines if the project is “actively maintained”.

Vulnerabilities **HIGH**
Determines if the project has open, known undefined vulnerabilities.

SAST **MEDIUM**
Determines if the project uses static code analysis tools.
OpenSSF Scorecard

Info how **YOU** want it

- Webviewer
- CLI tool
- GitHub action
score is 0: security policy file not detected

Remediation (click "Show more" below):

- Place a security policy file `SECURITY.md` in the root directory of your repository. This makes it easily discoverable by a vulnerability reporter.
- The file should contain information on what constitutes a vulnerability and a way to report it securely (e.g., issue tracker with private issue support, encrypted email with a published public key). Follow the coordinated vulnerability disclosure guidelines to respond to vulnerability disclosures.
- For GitHub, see more information [here](#).

Severity: Medium

Details:

Risk: **Medium** (possible insecure reporting of vulnerabilities)

This check tries to determine if the project has published a security policy. It works by looking for a file named `SECURITY.md` (case-insensitive) in a few well-known directories.

A security policy (typically a `SECURITY.md` file) can give users information about what constitutes a vulnerability and how to report one securely so that information about a bug is not publicly visible.

This check examines the contents of the security policy file awarding points for those policies that express vulnerability process(es), disclosure timelines, and have links (e.g., URL(s) and email(s)) to support the users.
Understand your dependencies

Your software and your users rely not only on the code you write, but also on the code your code depends on, the code that code depends on, and so on. An accurate view of the complete dependency graph is critical to understanding the state of your project. And it’s not just code: you need to know about security vulnerabilities, licenses, recent releases, and more.
<table>
<thead>
<tr>
<th>Package</th>
<th>Notes</th>
<th>Relation</th>
<th>License</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>absl-py</td>
<td>Direct</td>
<td></td>
<td>Apache-2.0</td>
<td>0</td>
</tr>
<tr>
<td>1.4.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>astunparse</td>
<td>Direct</td>
<td></td>
<td>non-standard</td>
<td>2</td>
</tr>
<tr>
<td>1.6.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>flatbuffers</td>
<td>Direct</td>
<td></td>
<td>Apache-2.0</td>
<td>0</td>
</tr>
<tr>
<td>23.5.26</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gast</td>
<td>Direct</td>
<td></td>
<td>BSD-3-Clause</td>
<td>0</td>
</tr>
<tr>
<td>0.4.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Package</td>
<td>Notes</td>
<td>Relation</td>
<td>License</td>
<td>Dependencies</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------</td>
<td>----------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>absl-py</td>
<td></td>
<td>Direct</td>
<td>Apache-2.0</td>
<td>0</td>
</tr>
<tr>
<td>1.4.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>astunparse</td>
<td></td>
<td>Direct</td>
<td>non-standard</td>
<td>2</td>
</tr>
<tr>
<td>1.6.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>flatbuffers</td>
<td></td>
<td>Direct</td>
<td>Apache-2.0</td>
<td>0</td>
</tr>
<tr>
<td>23.5.26</td>
<td>13 ADVISORIES</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gast</td>
<td></td>
<td>Direct</td>
<td>BSD-3-Clause</td>
<td>0</td>
</tr>
<tr>
<td>0.4.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Lesson 2
Monitoring supports action
Lesson 2
Monitoring supports action
More free tools!

- OSV (Open Source Vulnerabilities) or ecosystem-specific vulnerability monitoring
- Dependency update bots (Dependabot or Renovatebot)
A distributed vulnerability database for Open Source

An open, precise, and distributed approach to producing and consuming vulnerability information for open source.

Ecosystems

Linux  Alpine  Android  crates.io  Debian  Go  Linux  Maven  npm  NuGet  OSS-Fuzz  Packagist  PyPI  Rocky Linux  Ruby
A distributed vulnerability database for Open Source

An open, precise, and distributed approach to producing and consuming vulnerability information for open source.

Ecosystems

2286  3254  722  1174  9379  1586  13573  3864  11989  495  2929  2154  10781  919  717

Linux  Alpine  Android  crates.io  Debian  Go  Linux  Maven  npm  NuGet  OSS-Fuzz  Packagist  PyPI  Rocky Linux  Ruby
Use a dependency update tool to stay on top of these changes!

- Dependabot
- Renovatebot
Lesson 3
Messengers support success
Lesson 3
Messengers support success
Code contributions, but also...

- Communication!
- Awareness!
- Soft skills!
- Documentation!
- Community education!
- Helping others!
Code contributions, but also...

- Communication!
- Awareness!
- Soft skills!
- Documentation!
- Community education!
- Helping others!
Hi, I'd like to know if you might have interest on creating a Github Security Policy file for [redacted]. The project already has a very well defined security policy so the file would only allow users to get this information through github standard ways.

It will be shown in the Security Dashboard and in the about section of the project:

**About**

- [Readme](#)
- [Apache-2.0 license](#)
- [Security policy](#)
- 0 stars
- 0 watching
- 66 forks
This change got applied to 20 high-profile projects downstream.
Closing thoughts...
Just as risks can propagate through communities... so can proactive, positive actions!
THANK YOU

Special thanks to:
Asra Ali
Josie Anugerah
Jen Barnason
Joyce Brum
Michael Goddard
Eve Martin-Jones
Kara Olive
Yorkim Parmentier
Julie Qiu
Nicky Ringland
James Wetter
Nina Zakharenko