Stranger Danger:
Your JavaScript Attack Surface Just Got Bigger

Micah Silverman

Snyk

snyk

DevSecCon Chapter Leader

Java Developer
Since 1995

Node.js Developer
Since 2010

Author, blogger, speaker,
oss contributor

Leading DevSecOps
Acceleration @Snyk

Micah Silverman

Reach out on Twitter and say hi 👋

@afitnerd

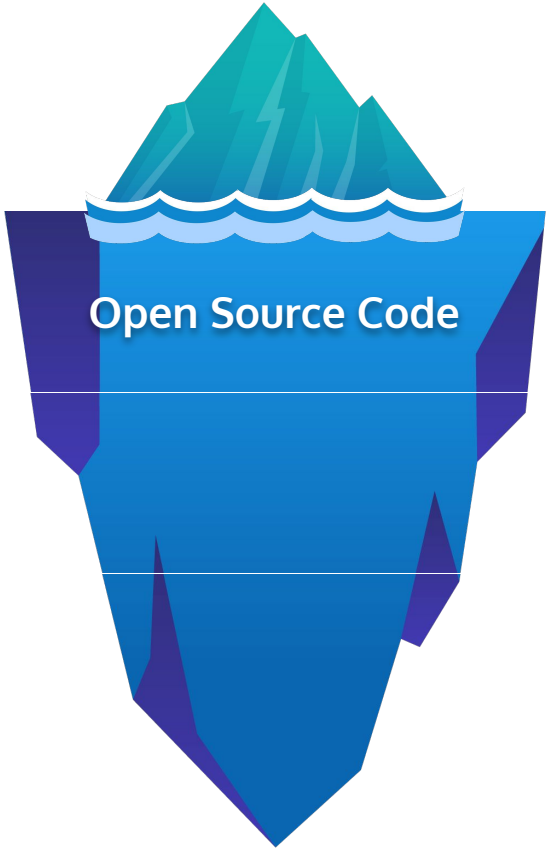
snyk

What is the future of open source software security?

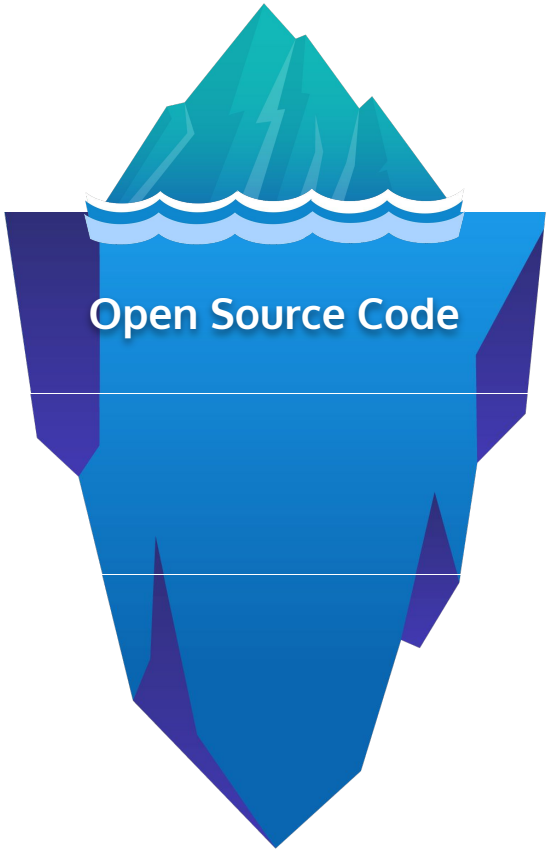

```
exports.admin = function (req, res, next) {

  User.find(
    {
       username: req.body.username,
       password: req.body.password
    },
    function (err, users) {}
  );
```


```
exports.admin = function (req, res, next) {

  User.find(
    {
       username: req.body.username,
       password: req.body.password
    },
    function (err, users) {}
  );
```

Security issues in this code?



- 80-90% of code-base is open-source
- 80% of vulnerabilities found in transitive dependencies



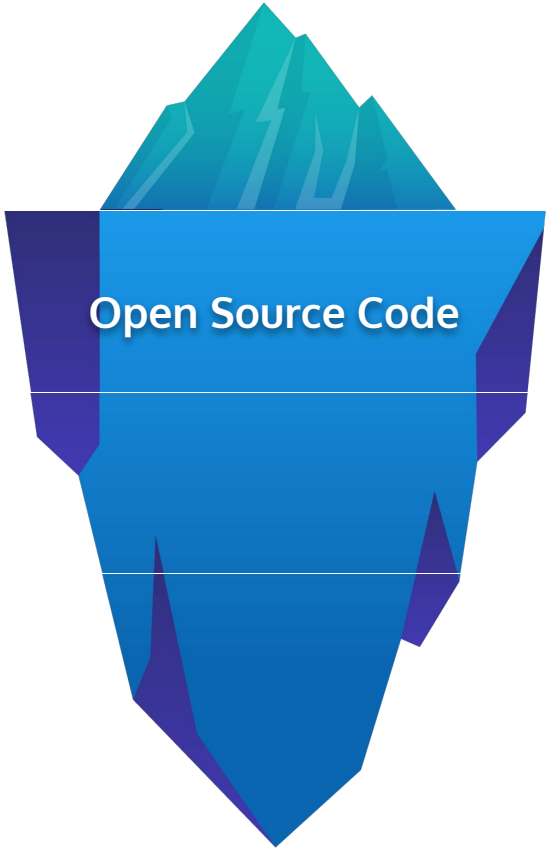

```
dust.escapeHtml = function(s) {
  if (typeof s === "string" {
    if (!HCHARS.test(s)) {
      return s;
    }

    return s.replace(QUOT,'&quot;').replace(SQUOT, '&#39;');
  }

  return s;
};
```

HIGH SEVERITY

644

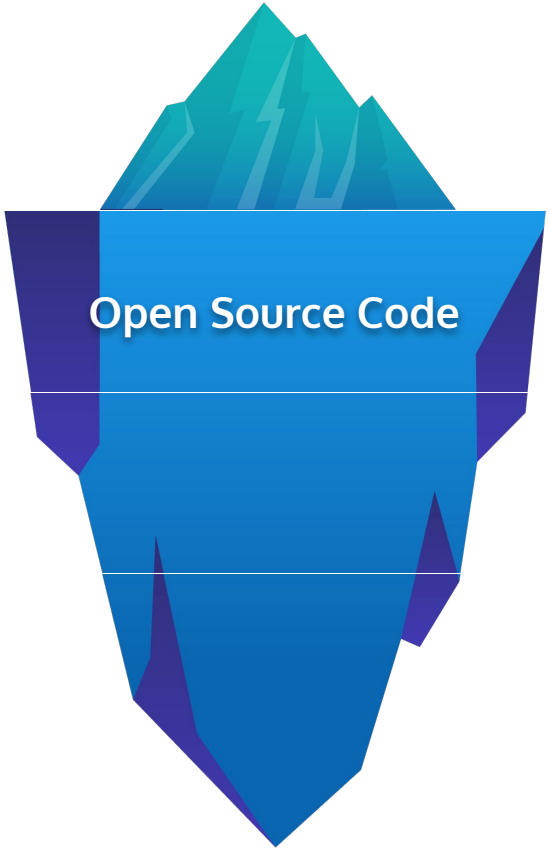
Code Injection

Vulnerable module:	dustjs-linkedin
Introduced through:	dustjs-linkedin@2.5.0
Exploit maturity:	No known exploit
Fixed in:	2.6.0



Your Code

```
const marked = require('marked');
app.locals.marked = marked;
```

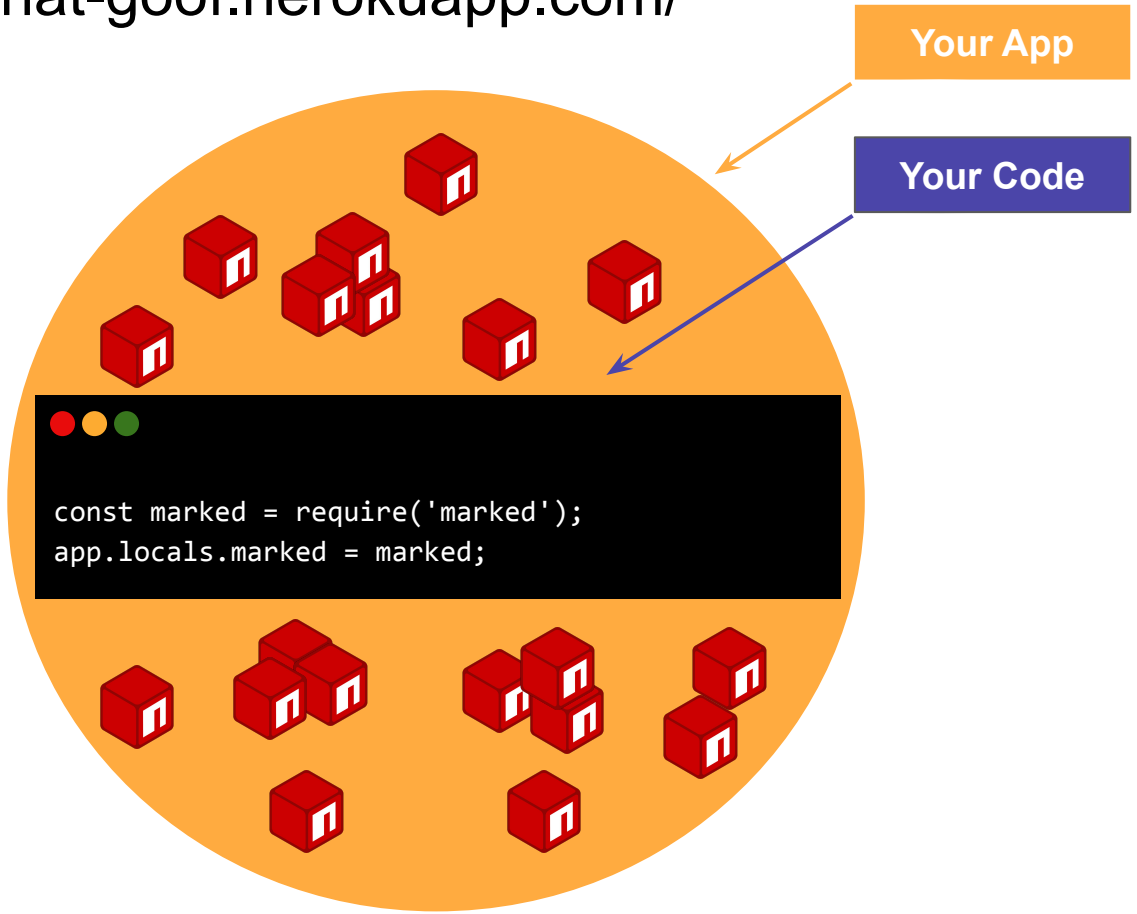


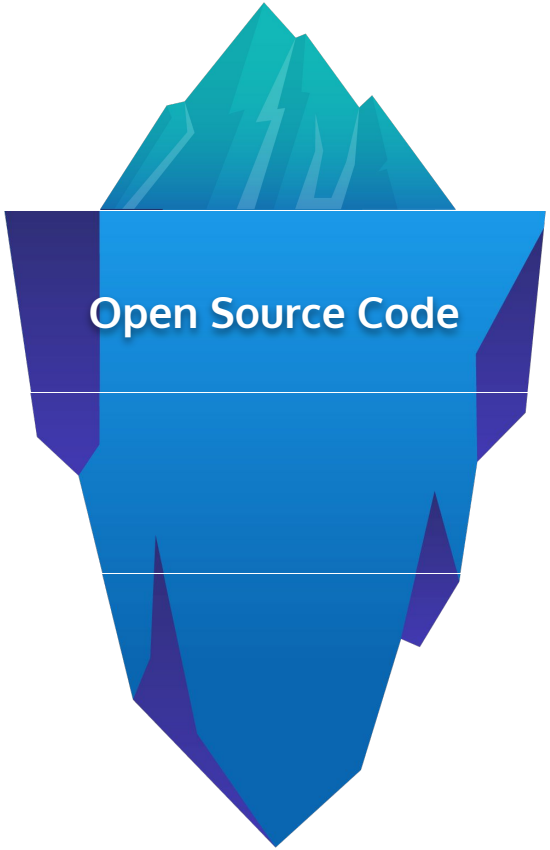
Your App

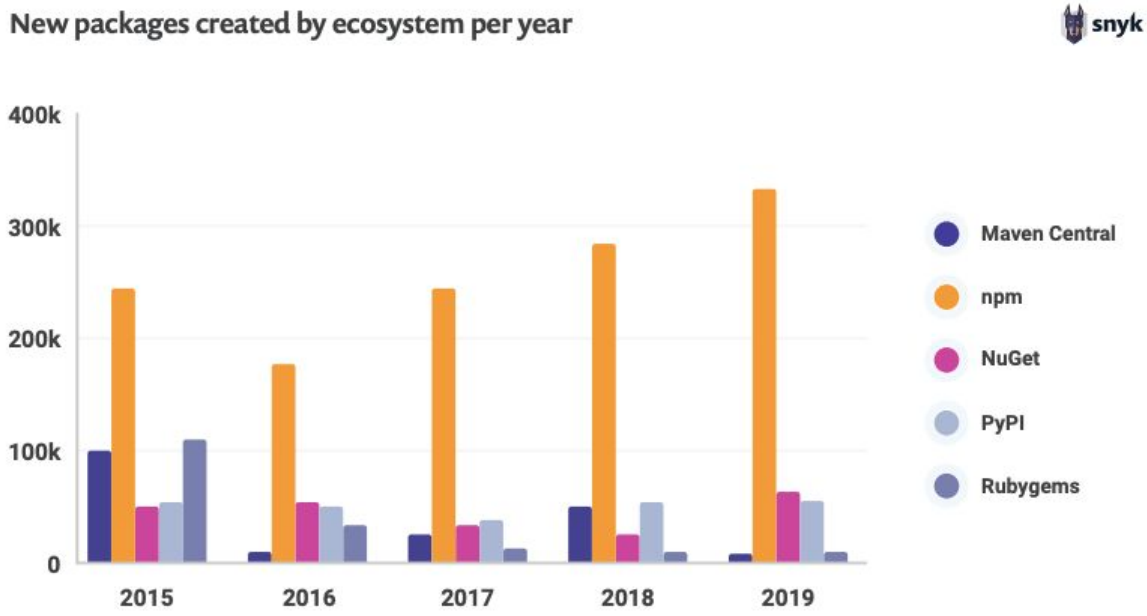
Your Code

```
const marked = require('marked');
app.locals.marked = marked;
```

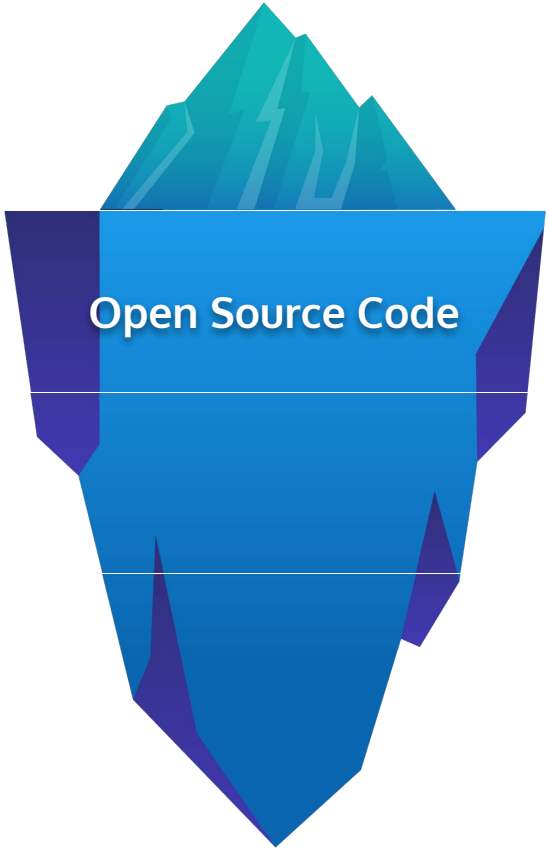
https://snyk-chat-goof.herokuapp.com/





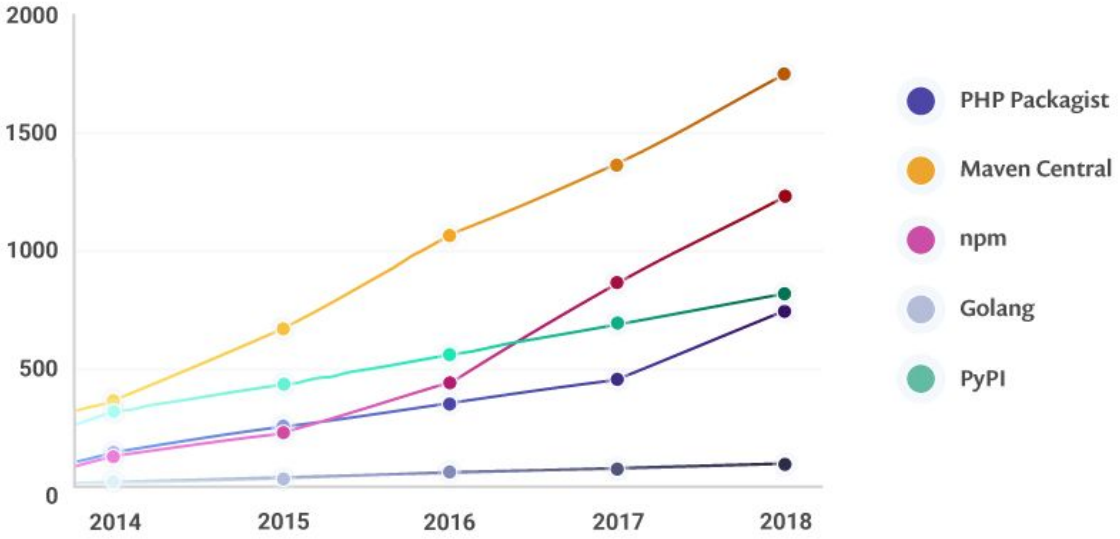


source: https://snyk.io/open-source-security

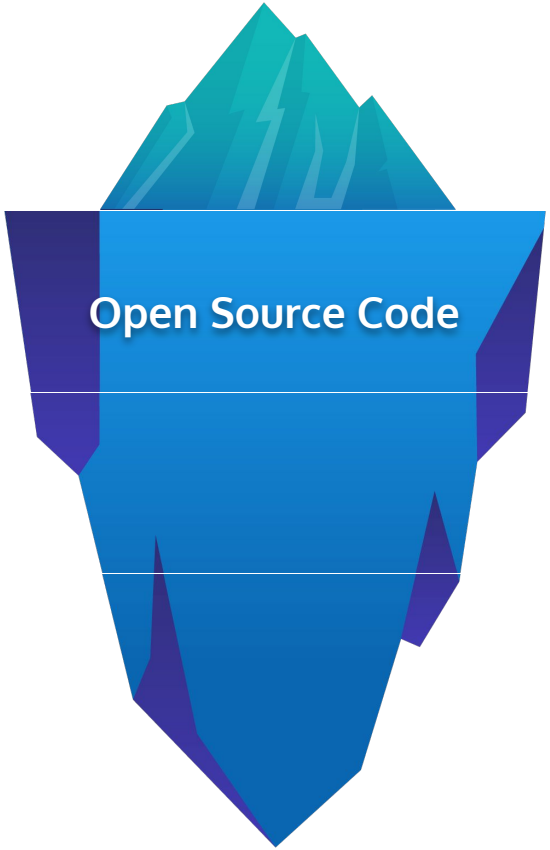


New vulnerabilities each year by ecosystem

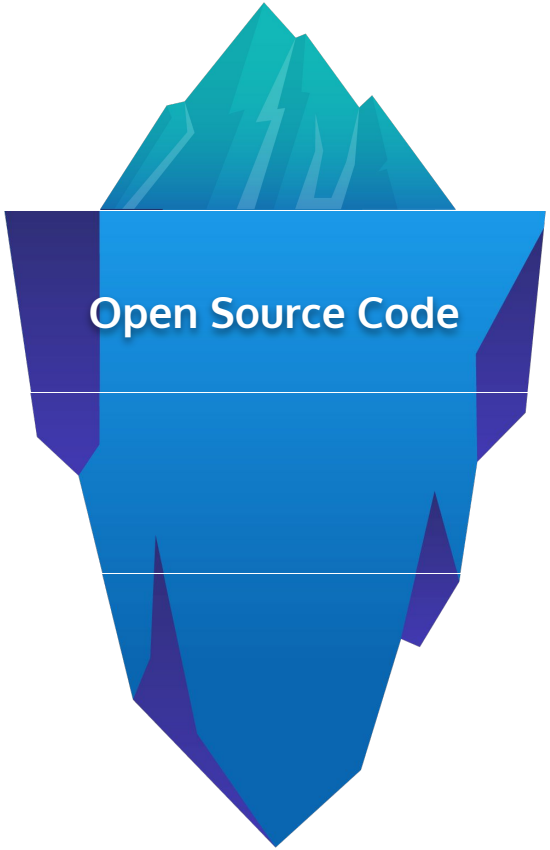
snyk



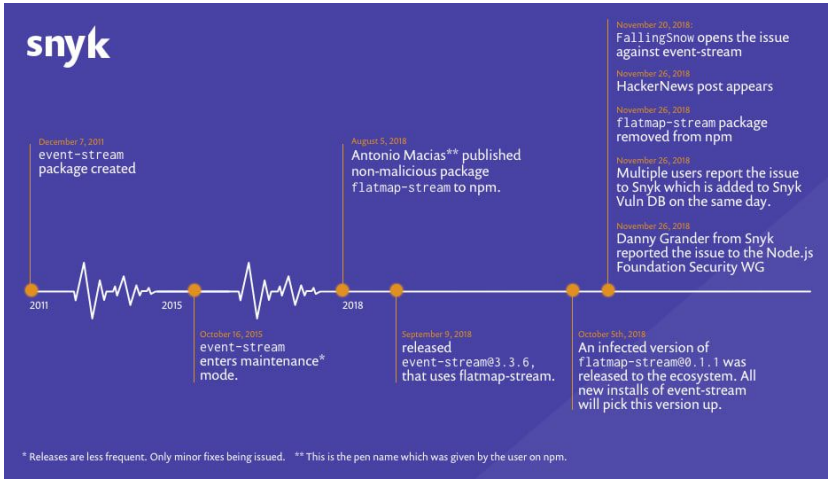
source: https://snyk.io/open-source-security

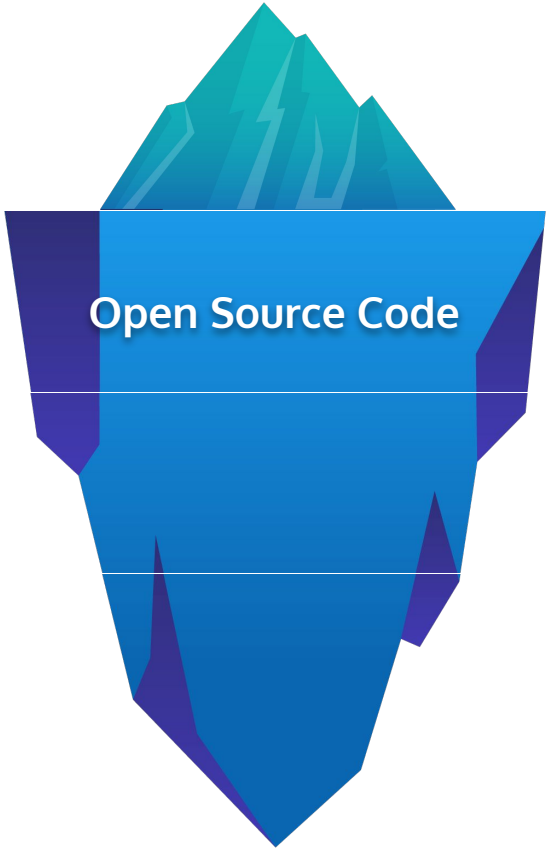


Open-Source Supply Chain Security



Open-Source Supply Chain Security

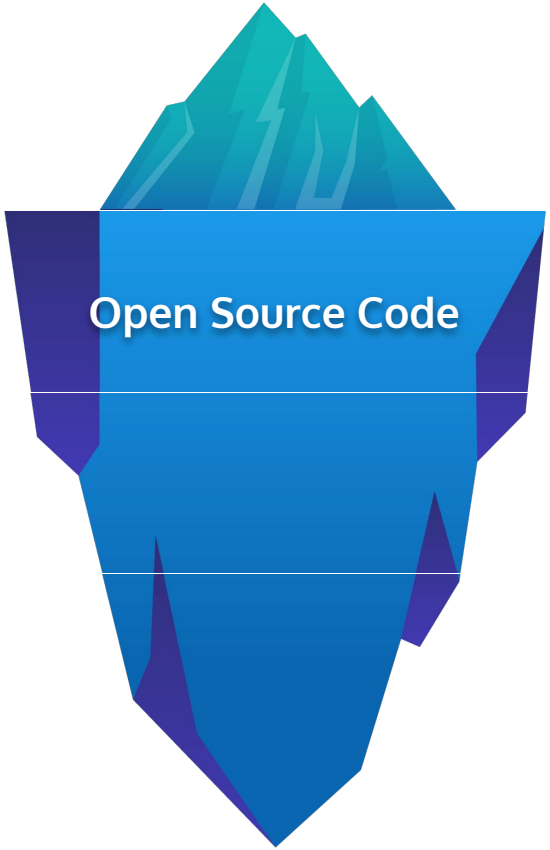




Open-Source Supply Chain Security

2019

💀 electron-native-notify



Open-Source Supply Chain Security

2019

💀 electron-native-notify

6 March 2019:
Non-malicious eletron-native-notify package is added to npm at version 1.0.0.

8 March 2019:
User sawlysawly added a commit that added the electron-native-notify dependency to the EasyDEX-GUI project at version "^1.1.5". EasyDEX-GUI is used by the Agama wallet which was affected.

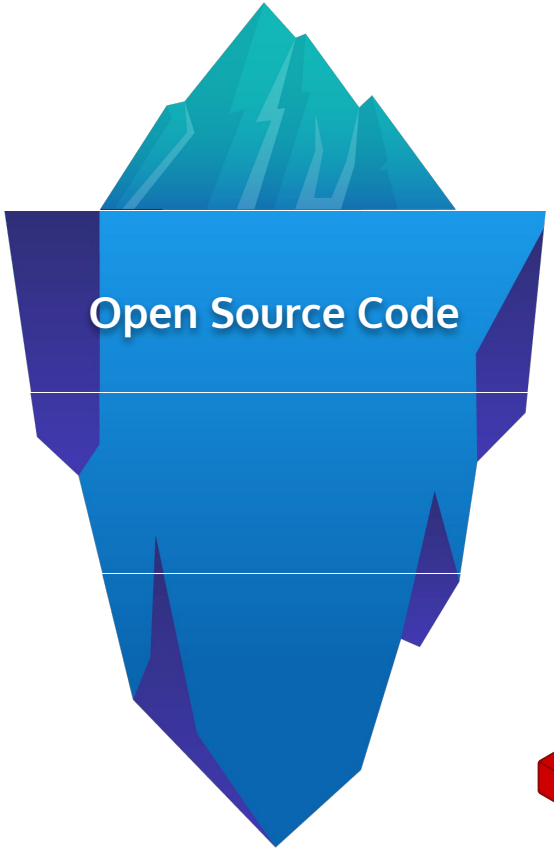
8 March 2019:
9 minor releases later, electron- native-notify v1.1.5 is published to npm

23 Mar 2019:
Malicious version of elec-tron-native-notify package published to npm at version 1.1.6

16 Apr - 11 May 2019:
The Agama Wallet is rebuilt and published, using the most recent version of the elec-tron-native-notify library, which at the time is 1.2.0

4 June 2019:
The npm security staff and Komodo removed the malicious dependency from the EasyDEX-GUI projects and pulled the package from npm, replacing it with a clean security version.

5 June 2019:
npm and Komodo publicly announce the security flaws to their users.



Open-Source Supply Chain Security

2020

urijs@1.18.12

Medium severity,
Improper Input Validation

2020

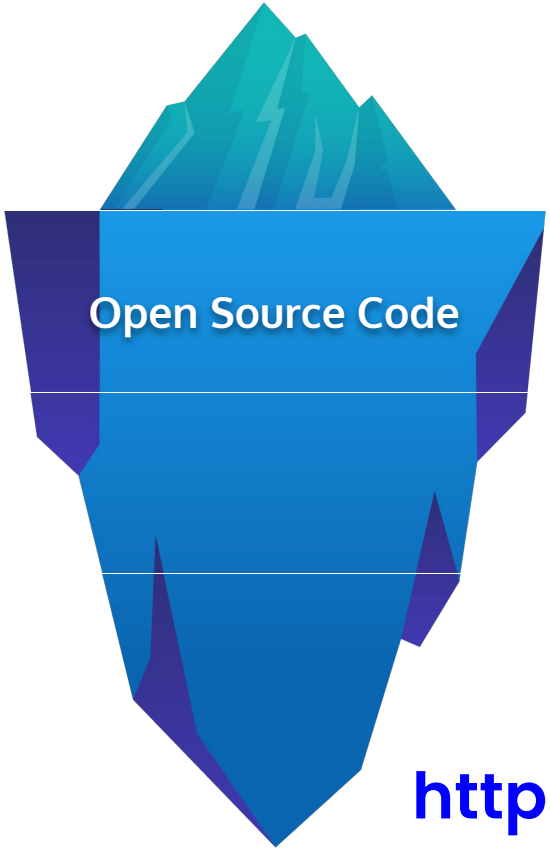
frappe-charts

Medium severity,
Cross-site Scripting (XSS)

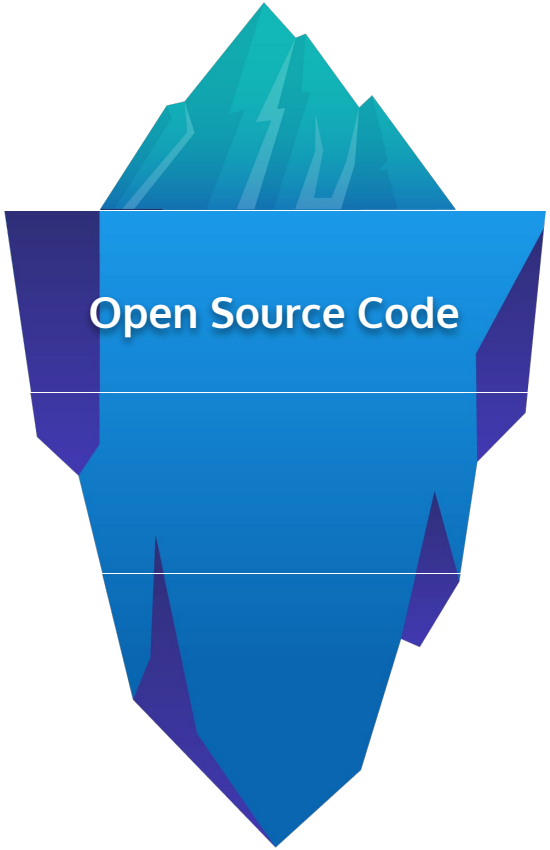
2021

ejs@*

High severity,
Arbitrary Code Injection



https://snyk-chat-goof.herokuapp.com



snyk Advisor | npm | Search packages | Open Source Basics | Ecosystem Insights | Code Securely | About Us | Sign Up

moment v2.29.1

Parse, validate, manipulate, and display dates

NPM README GitHub MIT Latest version published 4 months ago

```
npm install moment
```

Explore Similar Packages

date-fns 87 / 100 | torque 42 / 100 | movement 36 / 100

Package Health Score

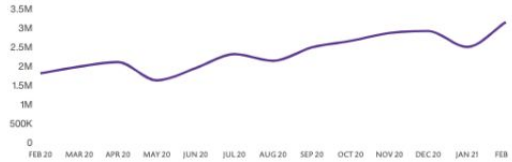
80 / 100

POPULARITY	KEY ECOSYSTEM PROJECT
MAINTENANCE	INACTIVE
SECURITY	NO KNOWN SECURITY ISSUES
COMMUNITY	ACTIVE

Make sure the open source you're using is safe to use — SECURE MY PROJECT

Popularity KEY ECOSYSTEM PROJECT

WEEKLY DOWNLOADS (17,789,231)



DEPENDENTS	GITHUB STARS	FORKS	CONTRIBUTORS
46.35K	45.38K	6.84K	420

The npm package moment receives a total of 17,789,231 downloads a week. As such, we scored moment popularity level to be Key ecosystem project.

Based on project statistics from the GitHub repository for the npm package moment, we found that it has been starred 45,380 times, and that 46,351 other projects in the ecosystem are dependent on it.

Downloads are calculated as moving averages for a period of the last 12 months, excluding weekends and known missing data points.

Maintenance INACTIVE

COMMIT FREQUENCY

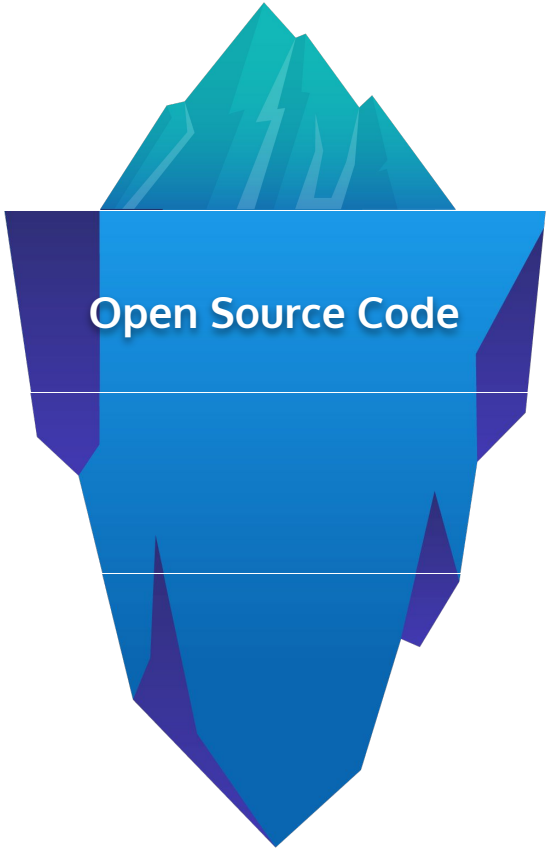
OPEN ISSUES	MERGED PR	OPEN PR	LAST COMMIT
87	707	31	3 months ago

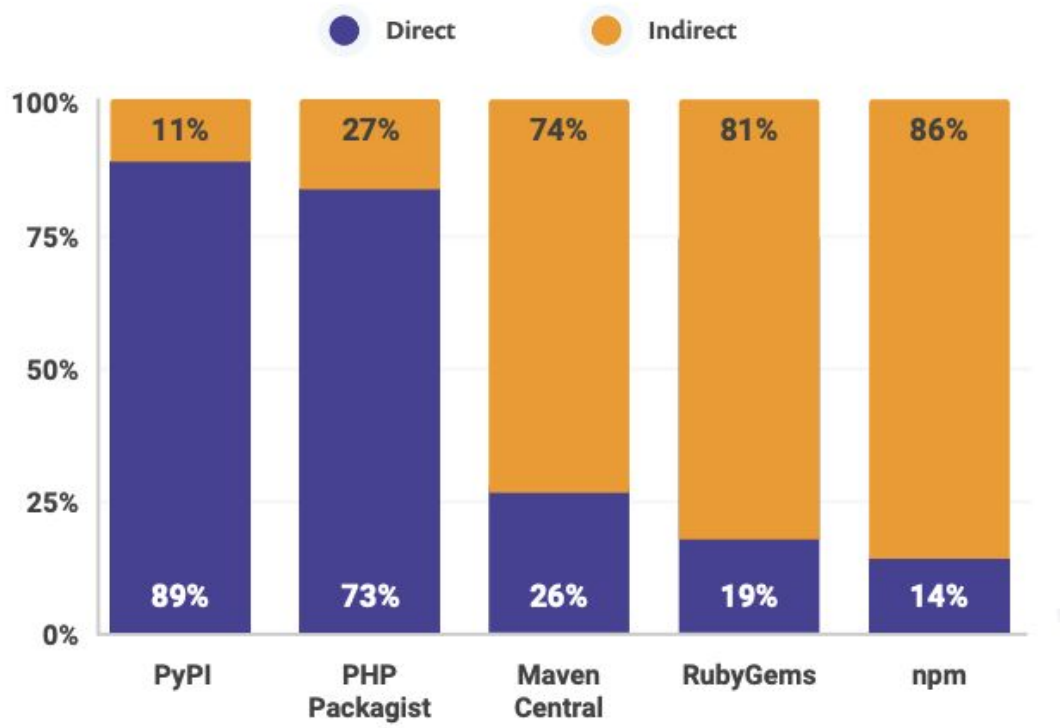
Further analysis of the maintenance status of moment based on released npm versions cadence, the repository activity, and other data points determined that its maintenance is Inactive.

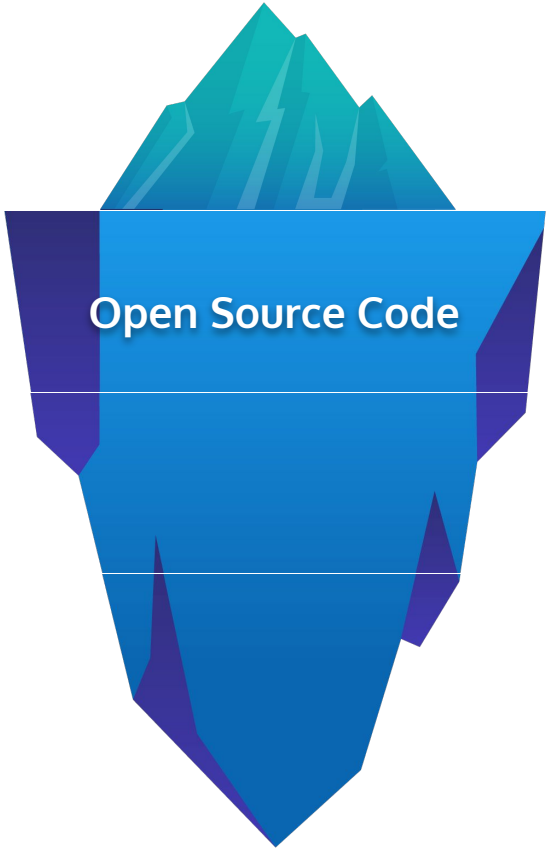
We found that moment demonstrates a positive version release cadence with at least one new version released in the past 12 months.

As a healthy sign for on-going project maintenance, we found that the GitHub repository had at least 1 pull request or issue interacted with by the community.

source: https://snyk.io/advisor/npm-package/moment


Open Source Code


Vulnerabilities from direct versus indirect dependencies
snyk
Direct
Indirect
100%
75%
50%
25%
0%
11%
27%
74%
81%
86%
89%
73%
26%
19%
14%
PyPI
PHP Packagist
Maven Central
RubyGems
npm



[Snyk] Security upgrade yargs from 15.3.0 to 16.0.0 #84

Merged **lirantal** merged 1 commit into `master` from `snyk-fix-5a6805b9b93cef9713156a9eaee504dc` on Nov 18, 2020

Conversation 1 · Commits 1 · Checks 6 · Files changed 1

snyk-bot commented on Nov 18, 2020 — Contributor

Snyk has created this PR to fix one or more vulnerable packages in the `npm` dependencies of this project.

merge advice | Review recommended

✨ Snyk has automatically assigned this pull request, set who gets assigned.

Changes included in this PR

- Changes to the following files to upgrade the vulnerable dependencies to a fixed version:
  - package.json

Vulnerabilities that will be fixed

With an upgrade:

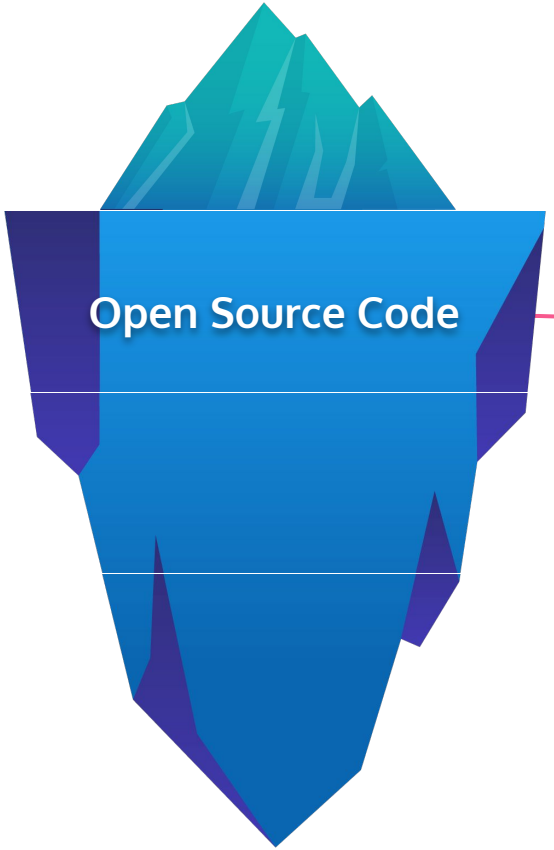
Severity	Priority Score (*)	Issue	Breaking Change	Exploit Maturity
H	758/1000 **Why?** Proof of Concept exploit, Recently disclosed, Has a fix available, CVSS 7.3	Prototype Pollution SNYK-JS-Y18N-1021887	Yes	Proof of Concept

Snyk app

Foot in the door with security of open-source dependencies

In a Cloud Native world, your app is more than your code

Your JavaScript App Attack Surface Just Got Bigger



https://app.snyk.io

snyk | Team Dagobah | Liran Tal

Dashboard | Reports | Projects | Integrations | Settings

Search projects… | Add project

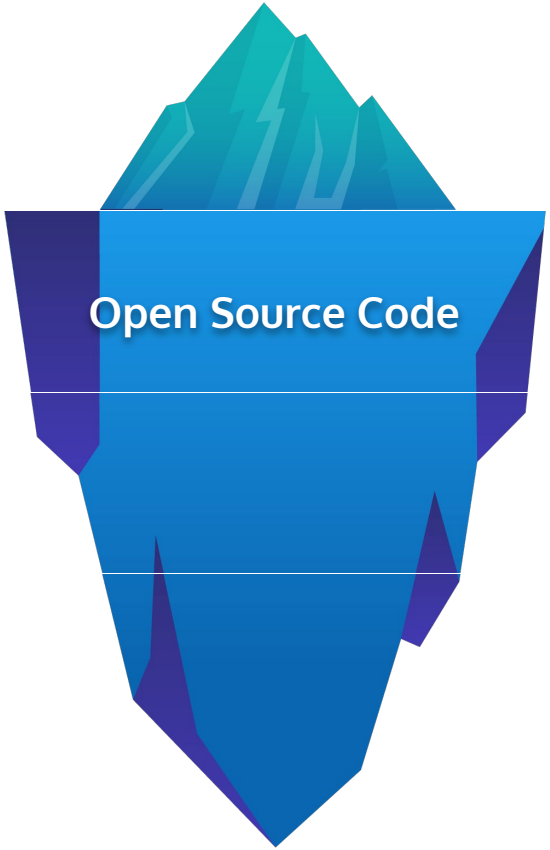
SHOW

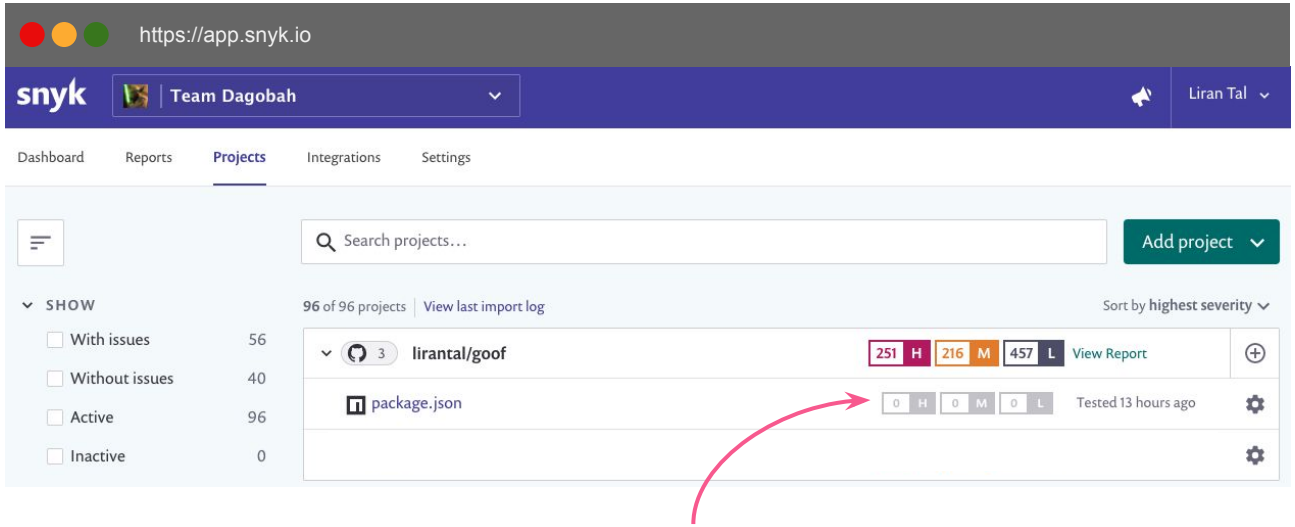
- With issues 56
- Without issues 40
- Active 96
- Inactive 0

96 of 96 projects | View last import log | Sort by highest severity

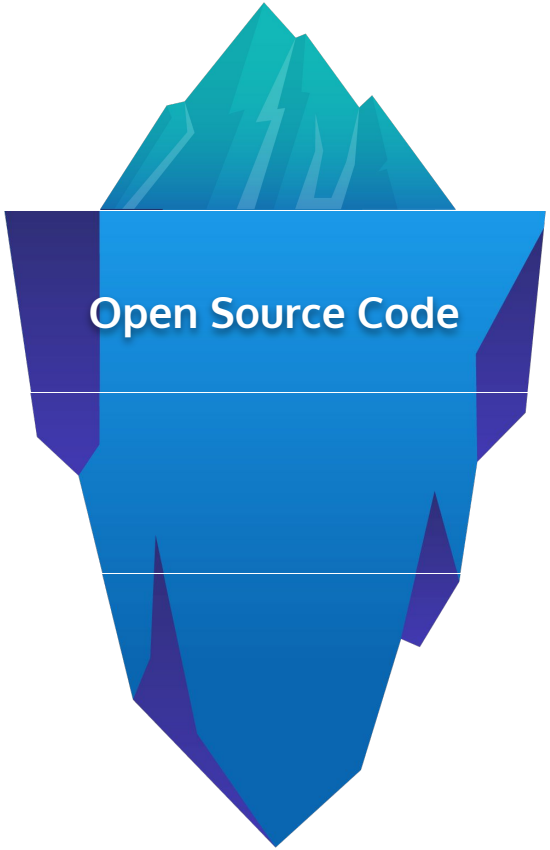
3 lirantal/goof — 251 H 216 M 457 L View Report

package.json — 33 H 25 M 5 L Tested 13 hours ago





App repository continuously scanned



https://app.snyk.io

snyk | Team Dagobah | Liran Tal

Dashboard | Reports | Projects | Integrations | Settings

Search projects… | Add project

SHOW

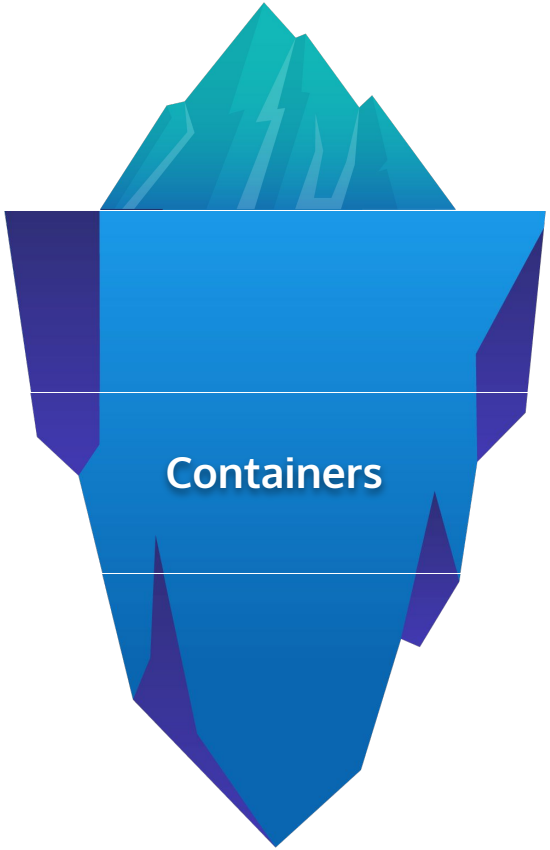
- With issues 56
- Without issues 40
- Active 96
- Inactive 0

96 of 96 projects | View last import log | Sort by highest severity

3 lirantal/goof — 251 H 216 M 457 L View Report

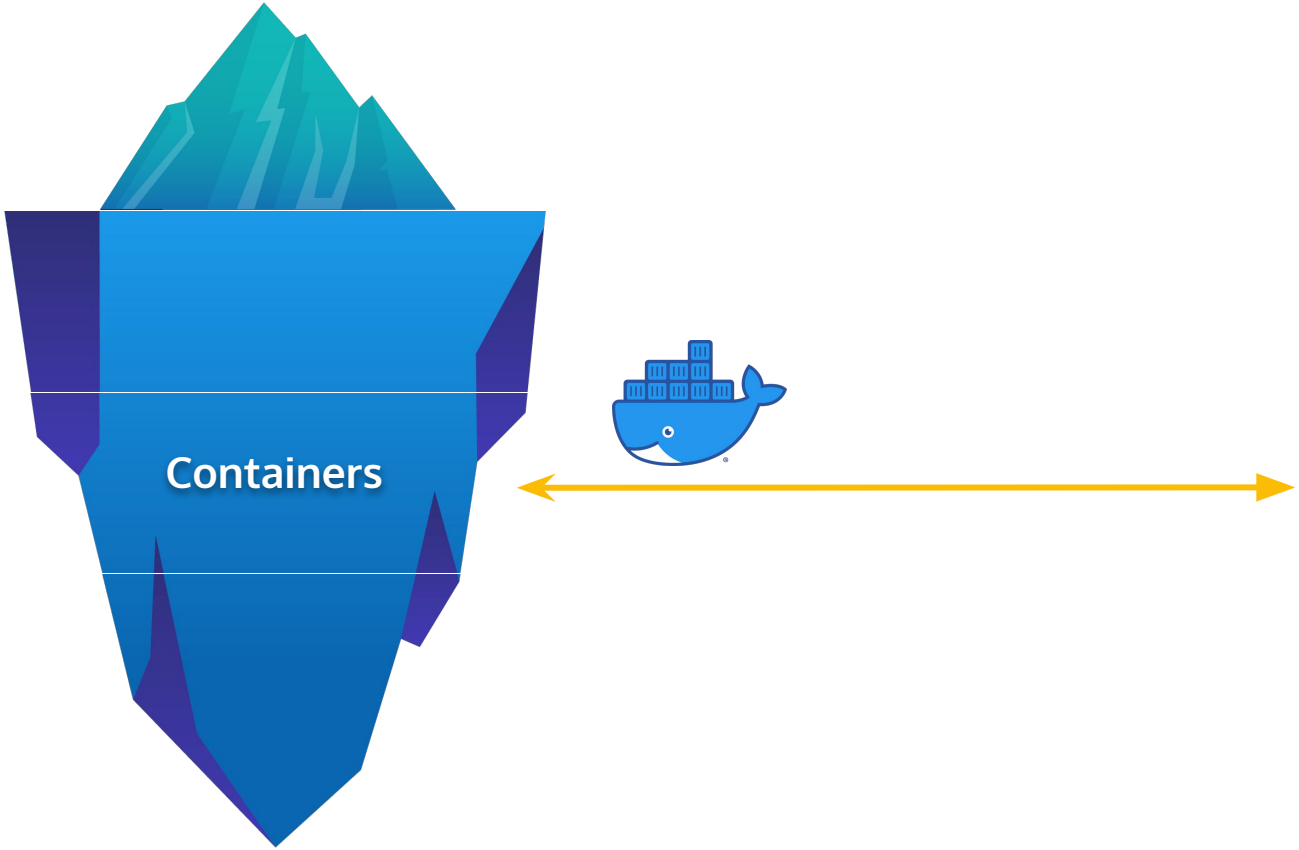
package.json — 0 H 0 M 0 L Tested 13 hours ago

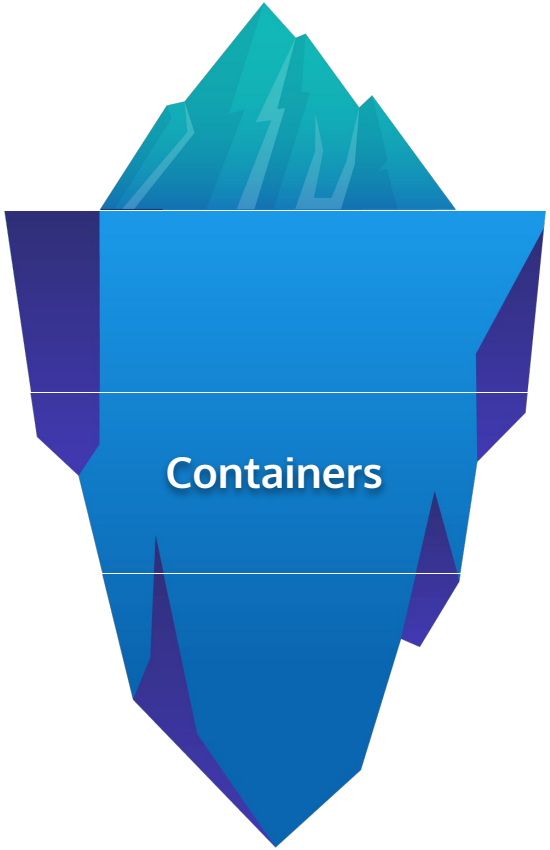
???


Containers


Containers, FaaS
& Static Sites

Vercel
netlify
AWS Lambda


Containers



https://app.snyk.io

snyk | Team Dagobah | Liran Tal

Dashboard | Reports | Projects | Integrations | Settings

Search projects…

Add project

SHOW

- With issues 56
- Without issues 40
- Active 96
- Inactive 0

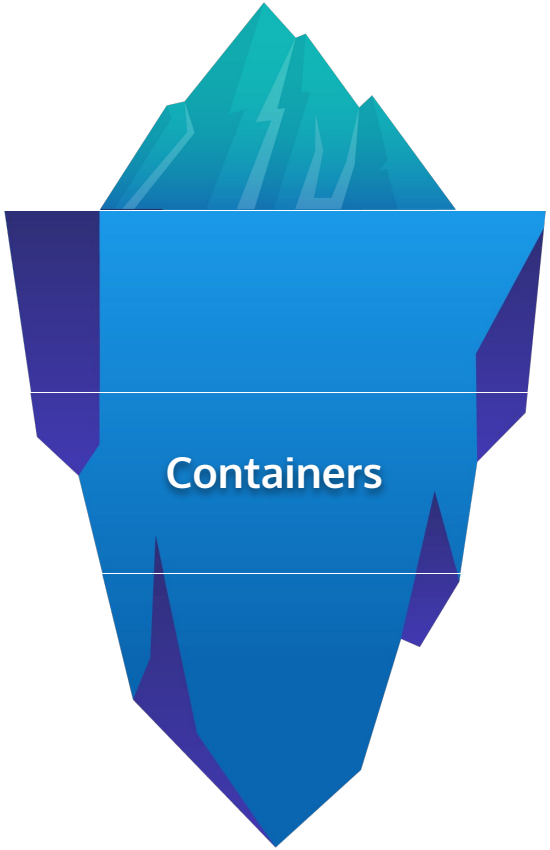
96 of 96 projects | View last import log

Sort by highest severity

3 lirantal/goof — 251 H, 216 M, 457 L, View Report

package.json — 0 H, 0 M, 0 L, Tested 13 hours ago

???



https://app.snyk.io

snyk | Team Dagobah | Liran Tal

Dashboard | Reports | Projects | Integrations | Settings

Search projects…

Add project

SHOW

- With issues 56
- Without issues 40
- Active 96
- Inactive 0

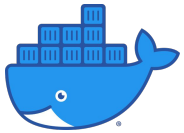
96 of 96 projects | View last import log

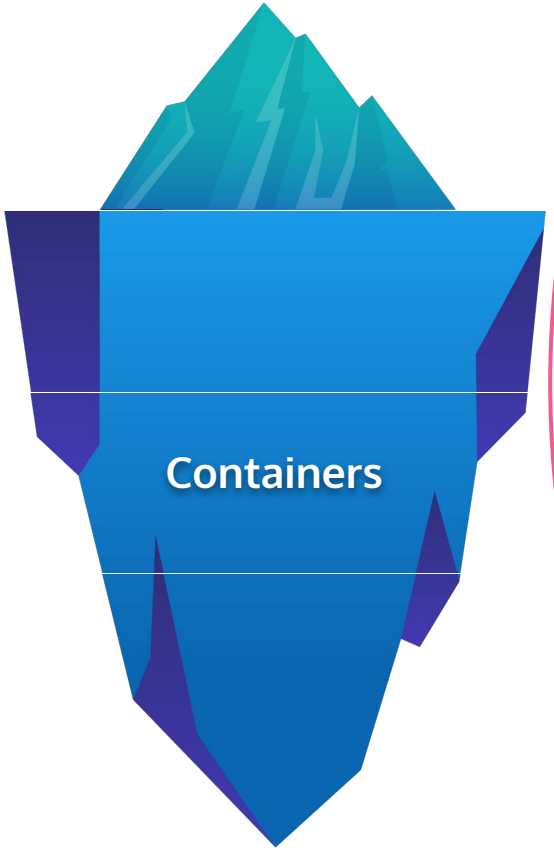
Sort by highest severity

3 lirantal/goof — 251 H, 216 M, 457 L — View Report

package.json — 0 H, 0 M, 0 L — Tested 13 hours ago

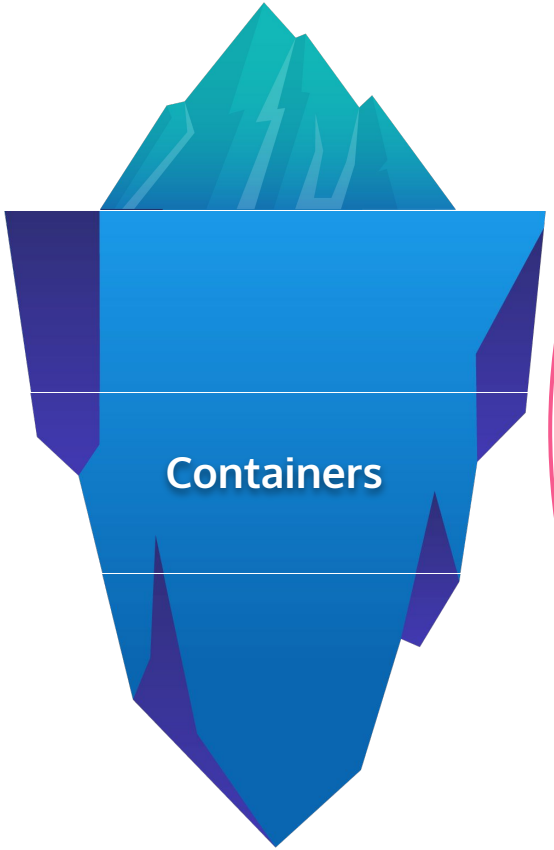
Dockerfile — 216 H, 187 M, 452 L — Tested 4 hours ago






```
FROM node

RUN apt-get update
RUN apt-get install -y imagemagick

COPY . /usr/src/goof
WORKDIR /usr/src/goof

RUN npm install

CMD ["npm", "start"]
```

Big image, many (vulnerable) libraries?



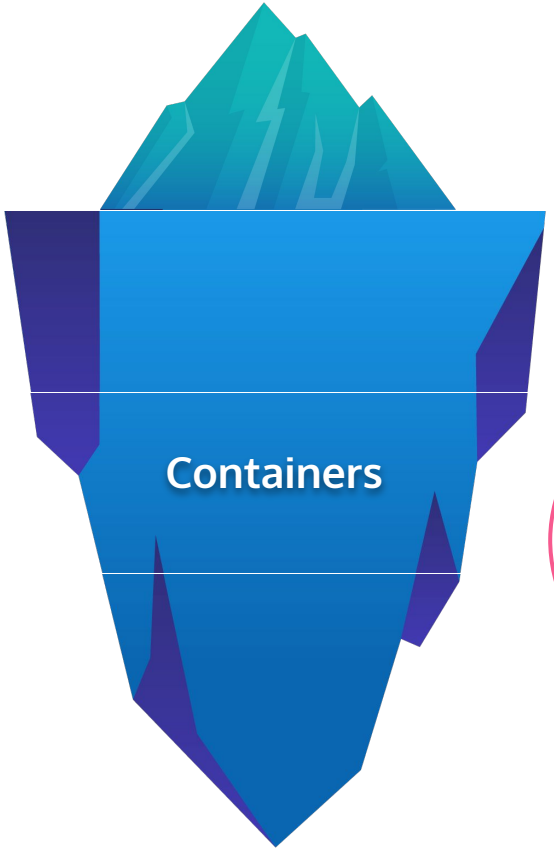

```
FROM node

RUN apt-get update
RUN apt-get install -y imagemagick

COPY . /usr/src/goof
WORKDIR /usr/src/goof

RUN npm install

CMD ["npm", "start"]
```

Common software vulnerable?

HIGH SEVERITY | EXPLOIT: MATURE

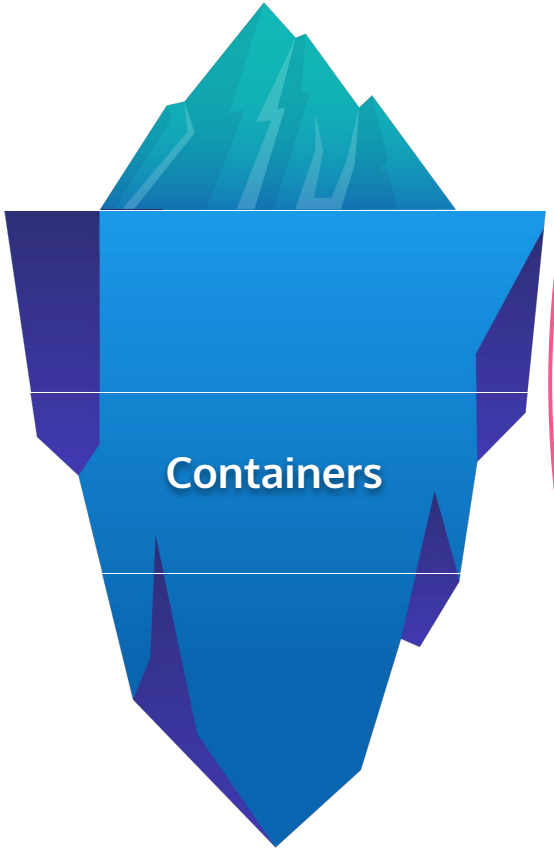
XML Injection

Vulnerable module:	imagemagick/libmagickwand-dev
Introduced through:	imagemagick/libmagickwand-dev@8:6.9.7.4+dfsg-11+deb9u7, and others
Exploit maturity:	Mature
Fixed in:	8:6.9.7.4+dfsg-11+deb9u11



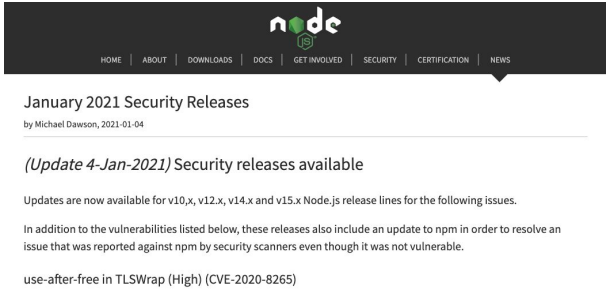

```
FROM node

RUN apt-get update
RUN apt-get install -y imagemagick

COPY . /usr/src/goof
WORKDIR /usr/src/goof

RUN npm install

CMD ["npm", "start"]
```

Dependencies vulnerable?



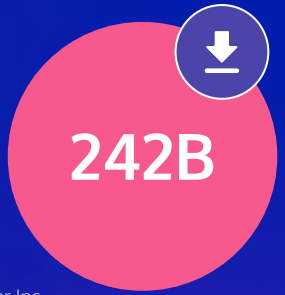

```
FROM node

RUN apt-get update
RUN apt-get install -y imagemagick

COPY . /usr/src/goof
WORKDIR /usr/src/goof

RUN npm install

CMD ["npm", "start"]
```

Runtime vulnerable?



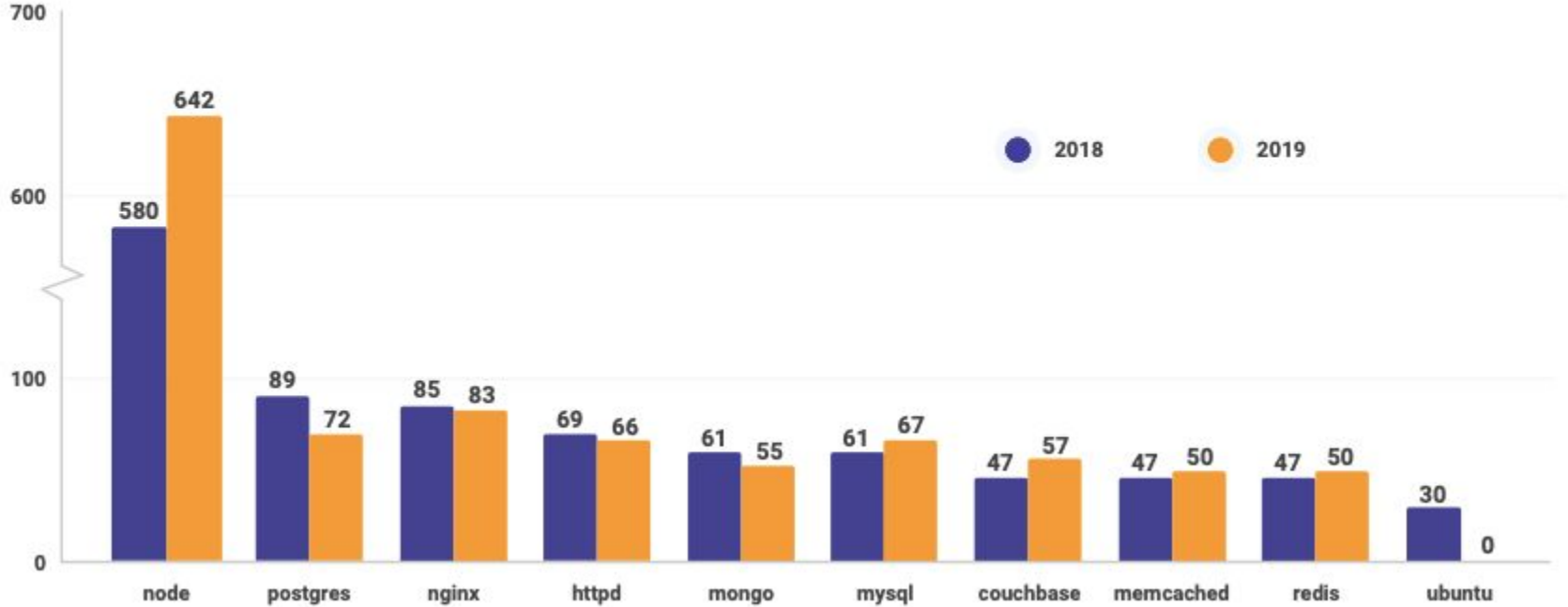
Digital transformation means rapid container adoption

Container downloads to date



Docker Inc

Vulnerabilities in official container images



source: https://snyk.io/open-source-security

Let’s hack a Node.js application!

Let’s hack a Node.js application!

we will exploit:

An Open Source Library

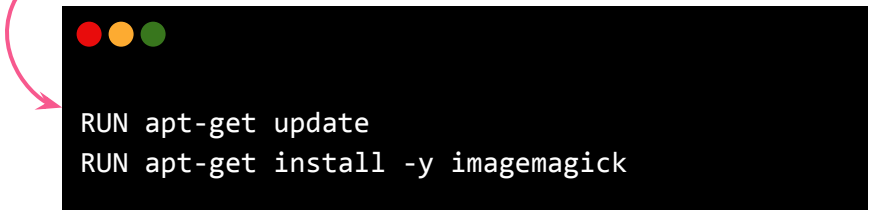
```
const marked = require('marked');
app.locals.marked = marked;

<div class="item">
  <a href="/edit/<%= todo._id %>">
      <%- marked(new String(todo.content)) %>
  </a>
</div>
```

Let’s hack a Node.js application!

we will exploit:

An Open Source Library

Container Common Software



Let’s hack a Node.js application!

we will exploit:

An Open Source Library

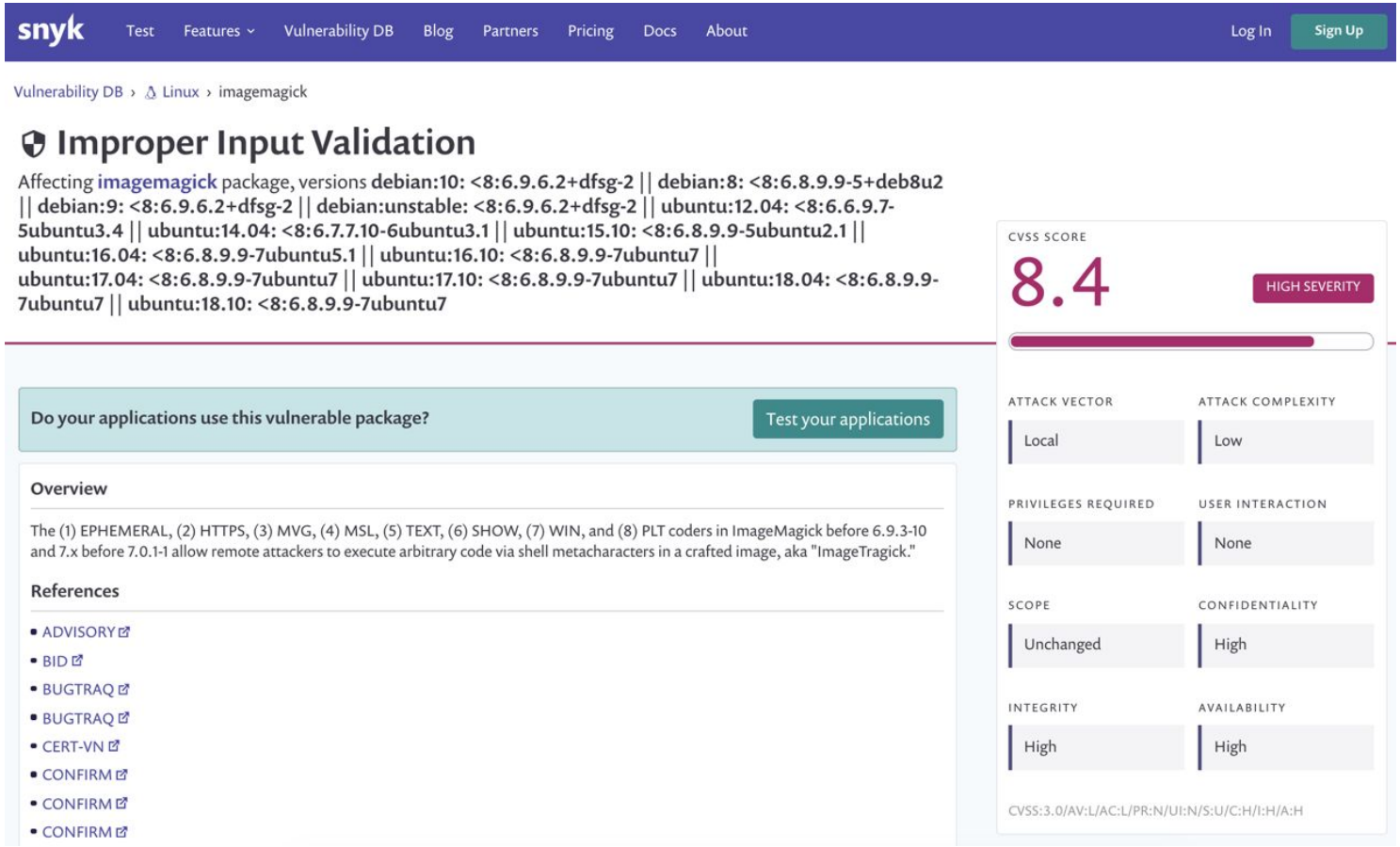
Container Common Software

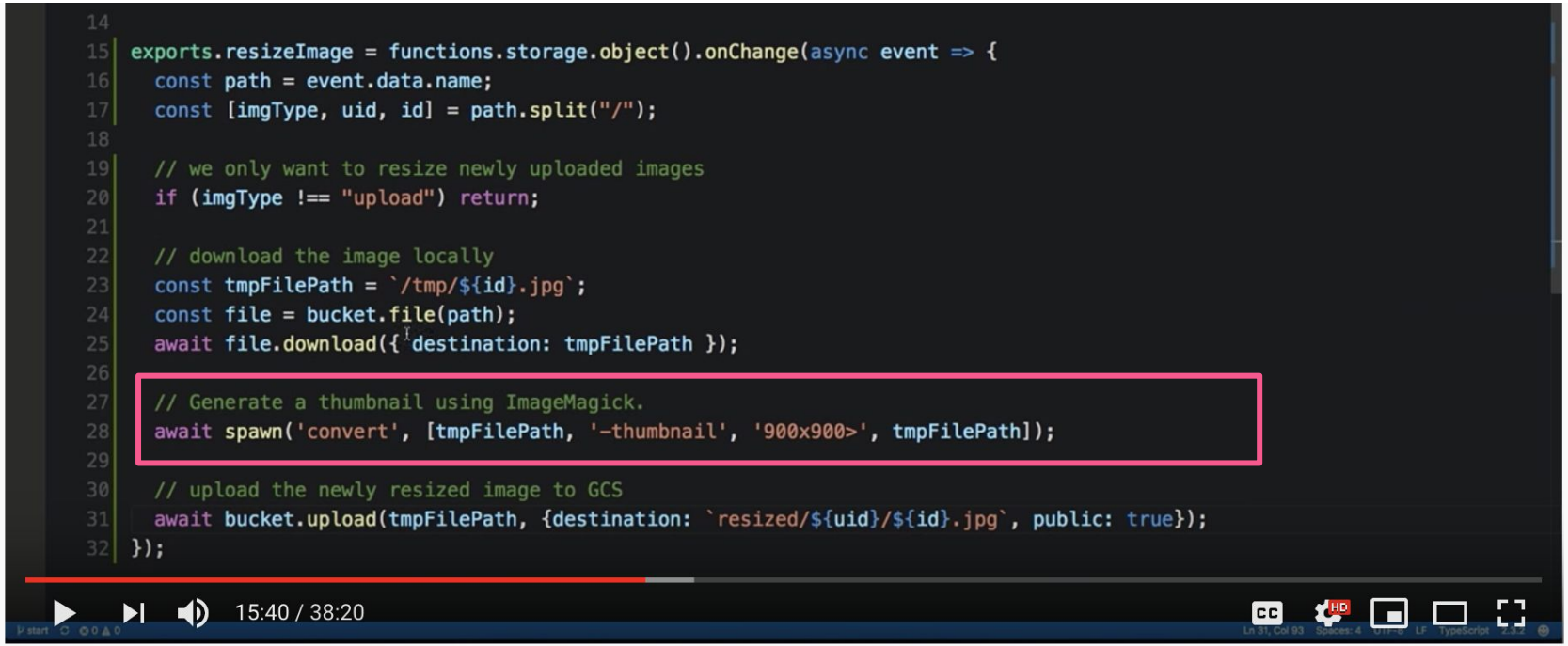
Container Node.js runtime

Woohoo
That was fun!

Woohoo
That was fun!

What can I do about it… ?


snyk
Test
Features
Vulnerability DB
Blog
Partners
Pricing
Docs
About
Log In
Sign Up
Vulnerability DB › Linux › imagemagick
Improper Input Validation
Affecting imagemagick package, versions debian:10: <8:6.9.6.2+dfsg-2 || debian:8: <8:6.8.9.9-5+deb8u2 || debian:9: <8:6.9.6.2+dfsg-2 || debian:unstable: <8:6.9.6.2+dfsg-2 || ubuntu:12.04: <8:6.6.9.7-5ubuntu3.4 || ubuntu:14.04: <8:6.7.7.10-6ubuntu3.1 || ubuntu:15.10: <8:6.8.9.9-5ubuntu2.1 || ubuntu:16.04: <8:6.8.9.9-7ubuntu5.1 || ubuntu:16.10: <8:6.8.9.9-7ubuntu7 || ubuntu:17.04: <8:6.8.9.9-7ubuntu7 || ubuntu:17.10: <8:6.8.9.9-7ubuntu7 || ubuntu:18.04: <8:6.8.9.9-7ubuntu7 || ubuntu:18.10: <8:6.8.9.9-7ubuntu7
CVSS SCORE
8.4
HIGH SEVERITY
ATTACK VECTOR
Local
ATTACK COMPLEXITY
Low
PRIVILEGES REQUIRED
None
USER INTERACTION
None
SCOPE
Unchanged
CONFIDENTIALITY
High
INTEGRITY
High
AVAILABILITY
High
CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Do your applications use this vulnerable package?
Test your applications
Overview
The (1) EPHEMERAL, (2) HTTPS, (3) MVG, (4) MSL, (5) TEXT, (6) SHOW, (7) WIN, and (8) PLT coders in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allow remote attackers to execute arbitrary code via shell metacharacters in a crafted image, aka "ImageTragick."
References
ADVISORY
BID
BUGTRAQ
BUGTRAQ
CERT-VN
CONFIRM
CONFIRM
CONFIRM

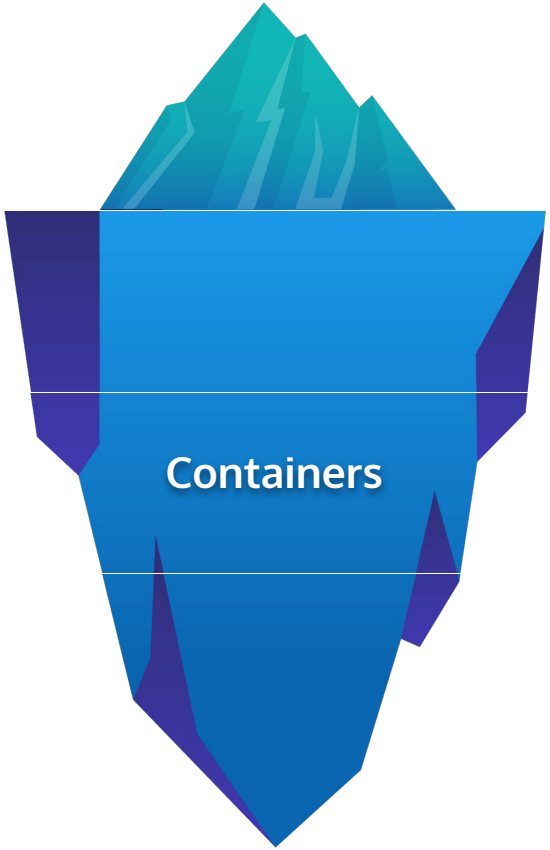


#io17 #GoogleIO #GoogleIO2017

Build Modern Apps with Firebase and Google Cloud Platform (Google I/O '17)

18,358 views • May 17, 2017

220 8 SHARE SAVE



https://app.snyk.io

MEDIUM SEVERITY

514

Improper Input Validation

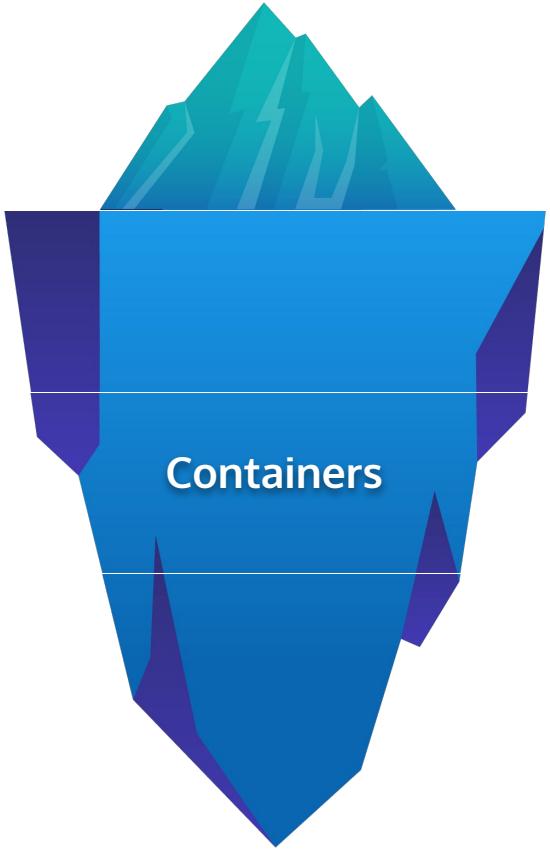
Vulnerable module:	imagemagick/libmagickwand-dev
Introduced through:	imagemagick/libmagickwand-dev@8:6.8.9.9-5+deb8u12, imagemagick/libmagickcore-dev@8:6.8.9.9-5+deb8u12 and others
Exploit maturity:	No known exploit
Fixed in:	8:6.8.9.9-5+deb8u16
Dockerfile instruction:	RUN apt-get install -y imagemagick

Detailed paths

- **Introduced through:** lirantal/docker-goof:latest@latest › imagemagick/libmagickwand-dev@8:6.8.9.9-5+deb8u12
- **Introduced through:** lirantal/docker-goof:latest@latest › imagemagick/libmagickcore-dev@8:6.8.9.9-5+deb8u12
- **Introduced through:** lirantal/docker-goof:latest@latest › imagemagick@8:6.8.9.9-5+deb8u12

…and 20 more

Layer-level Docker vulnerabilities



https://app.snyk.io

snyk S.H.I.E.L.D.

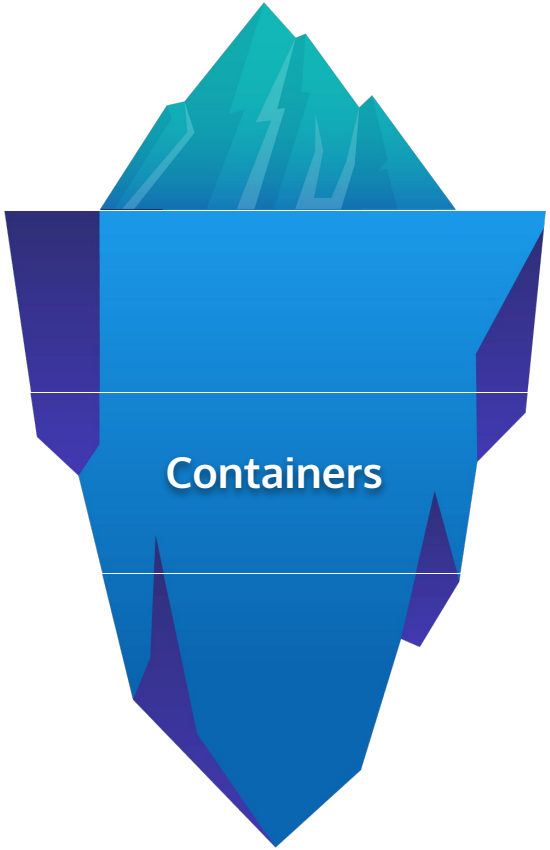
docker-image|node

Snapshot taken by recurring test 5 hours ago.

Vulnerabilities:	862 via 7657 paths	**Dependencies:**	383
Taken by:	Recurring	**Hostname:**	Lirans-MBP
Image ID:	2a78ab879533	**Image tag:**	10.4.0
Runtime:	docker 19.03.2	**Imported by:**	**Liran Tal** liran@snyk.io

862 vulnerabilities in node:10.4.0

Total node image tags: **3867**



https://app.snyk.io

snyk | S.H.I.E.L.D.

docker-image|node

Actionable Recommendation

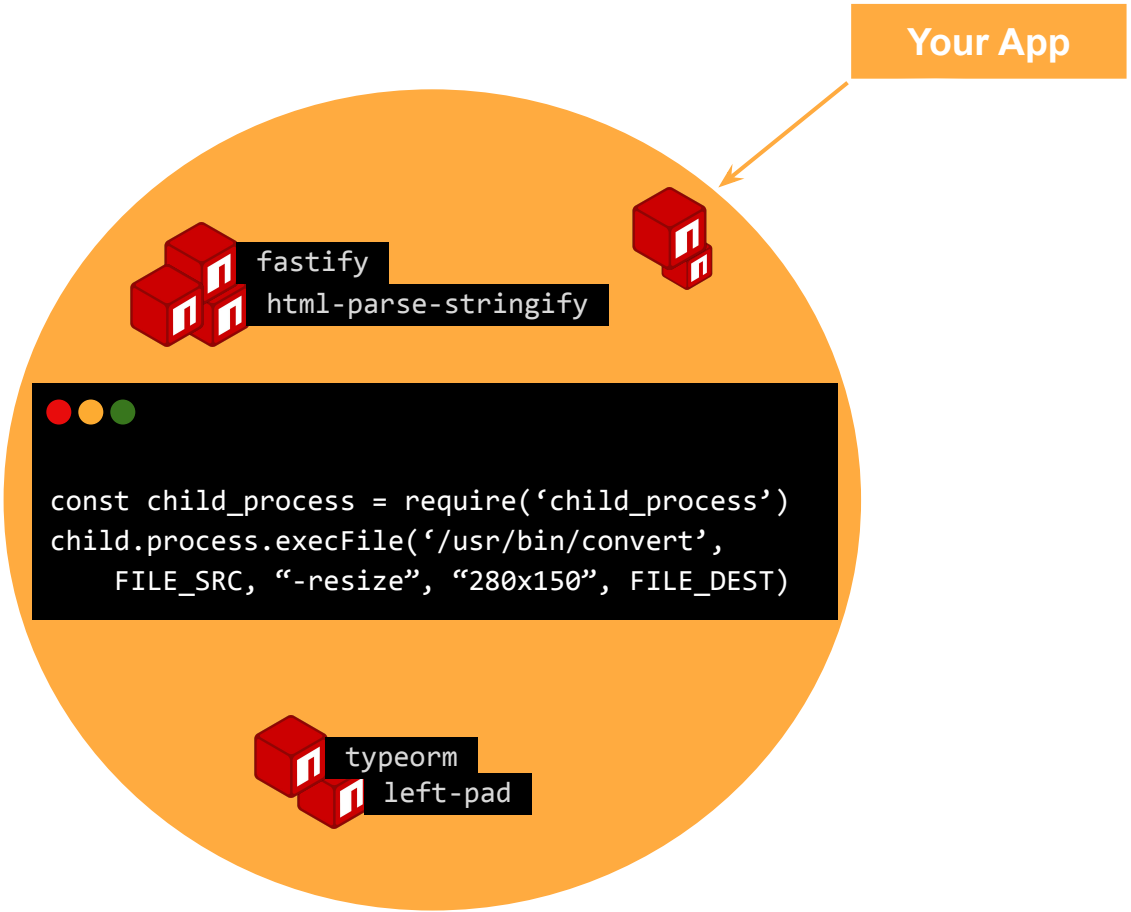
Snapshot taken by recurring test 5 hours ago.

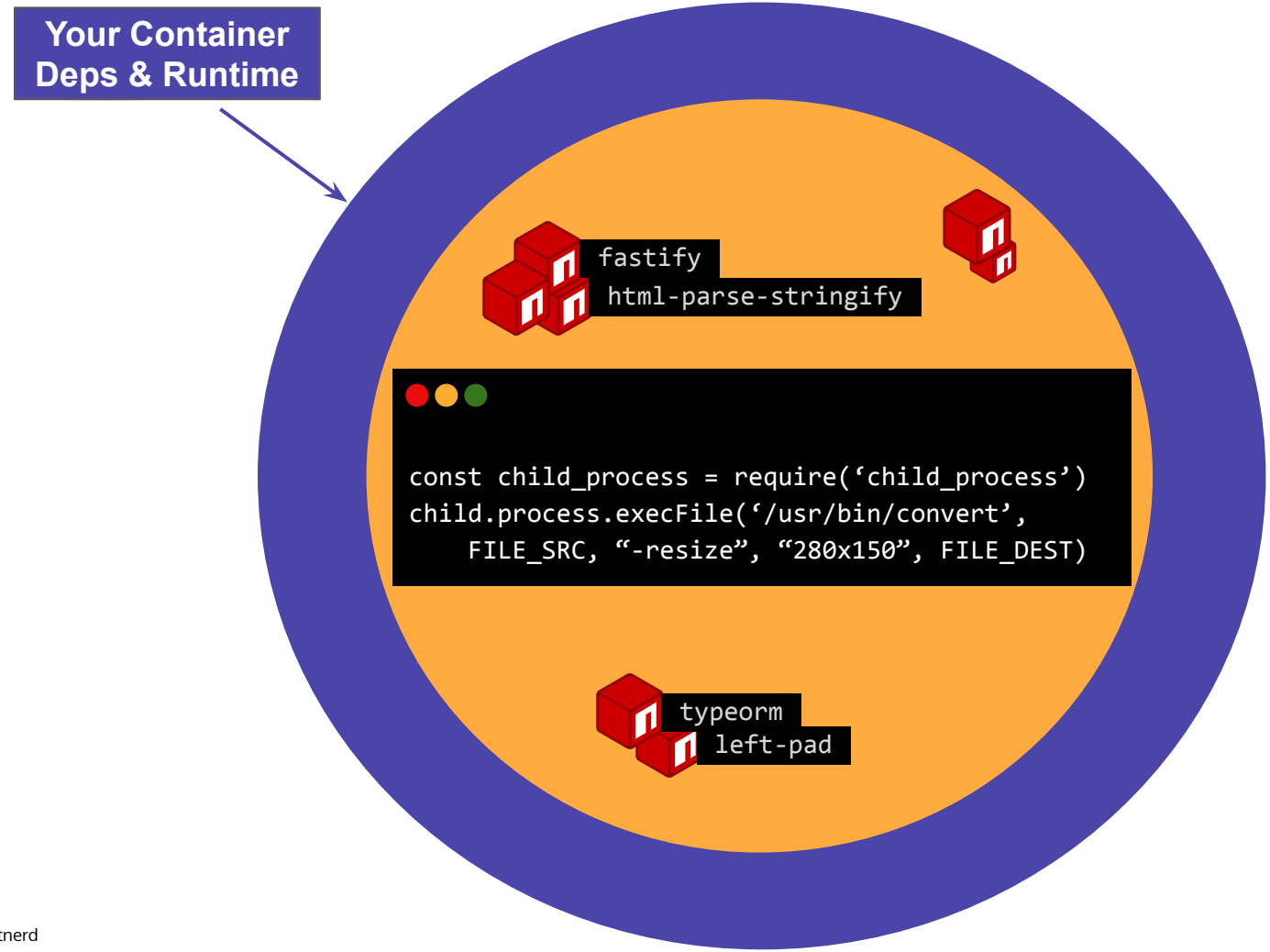
Vulnerabilities:	862 via 7657 paths	**Dependencies:**	383
Taken by:	Recurring	**Hostname:**	Lirans-MBP
Image ID:	2a78ab879533	**Image tag:**	10.4.0
Runtime:	docker 19.03.2	**Imported by:**	**Liran Tal** liran@snyk.io

Recommendations for base image upgrade

	BASE IMAGE	VULNERABILITIES	SEVERITY
Current image	node:10.4.0	862	390 high, 451 medium, 2
Minor upgrades	node:10.16.0	633	256 high, 356 medium, 2
Major upgrades	node:12.12.0	598	244 high, 339 medium, 1
Alternative upgrades	node:10.16.3-buster-slim	54	20 high, 26 medium, 8 lo

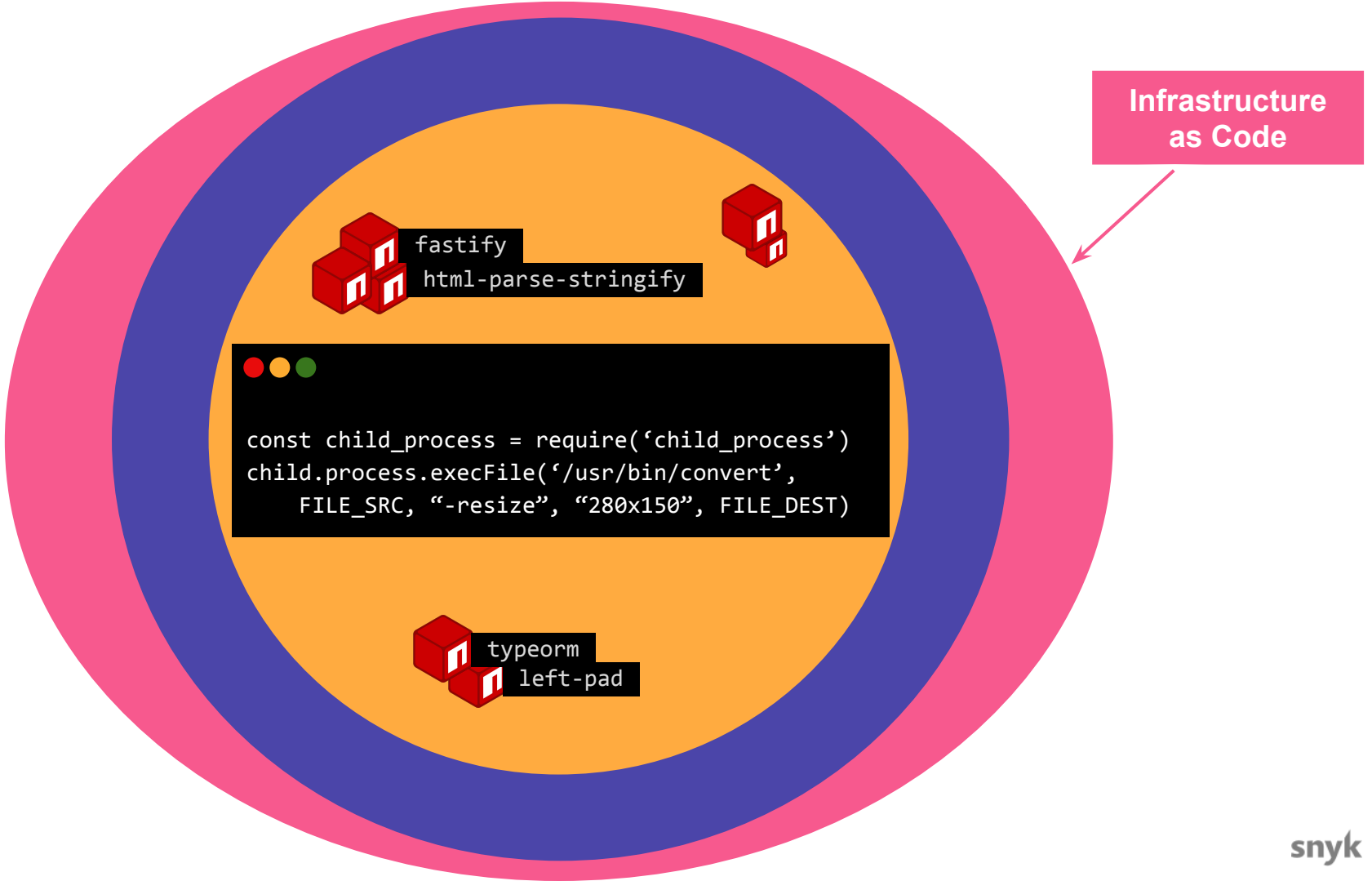

Your Code
const child_process = require(‘child_process’)
child.process.execFile(‘/usr/bin/convert’,
FILE_SRC, “-resize”, “280x150”, FILE_DEST)


Your App
fastify
html-parse-stringify
const child_process = require('child_process')
child.process.execFile('/usr/bin/convert',
FILE_SRC, "-resize", "280x150", FILE_DEST)
typeorm
left-pad

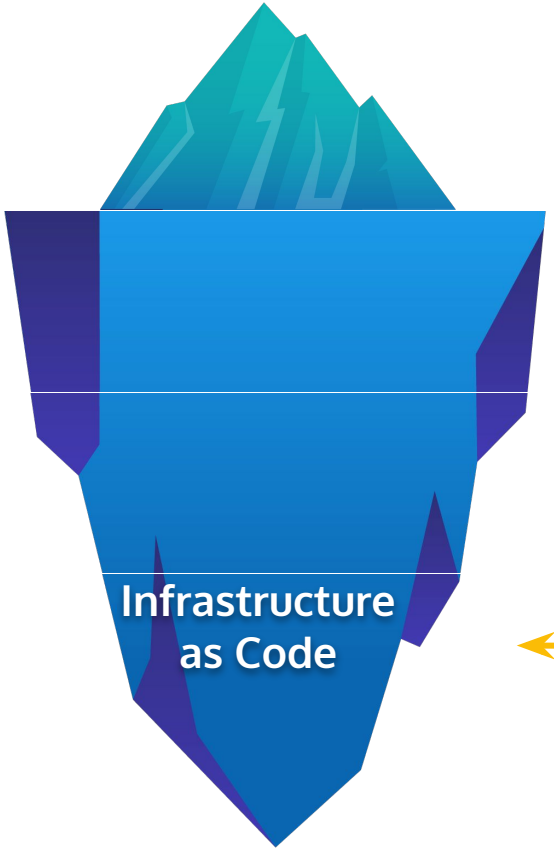

Your Container
Deps & Runtime
fastify
html-parse-stringify
const child_process = require('child_process')
child.process.execFile('/usr/bin/convert',
FILE_SRC, "-resize", "280x150", FILE_DEST)
typeorm
left-pad


fastify
html-parse-stringify
const child_process = require('child_process')
child.process.execFile('/usr/bin/convert',
FILE_SRC, "-resize", "280x150", FILE_DEST)
typeorm
left-pad

What else????


Infrastructure as Code
fastify
html-parse-stringify
const child_process = require('child_process')
child.process.execFile('/usr/bin/convert',
FILE_SRC, "-resize", "280x150", FILE_DEST)
typeorm
left-pad

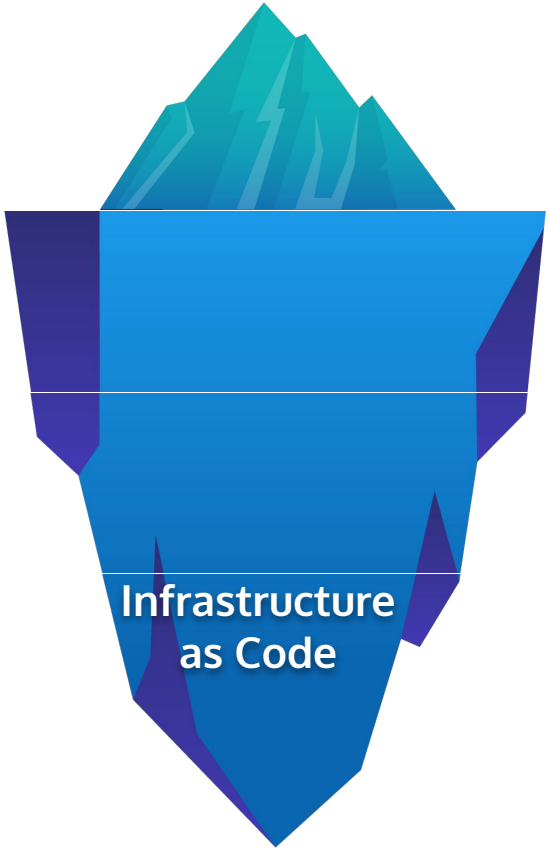

Infrastructure as Code
$ docker-compose up
$ kubectl apply -f node-app-deployment.yml
$ firebase deploy
$ netlify deploy --prod



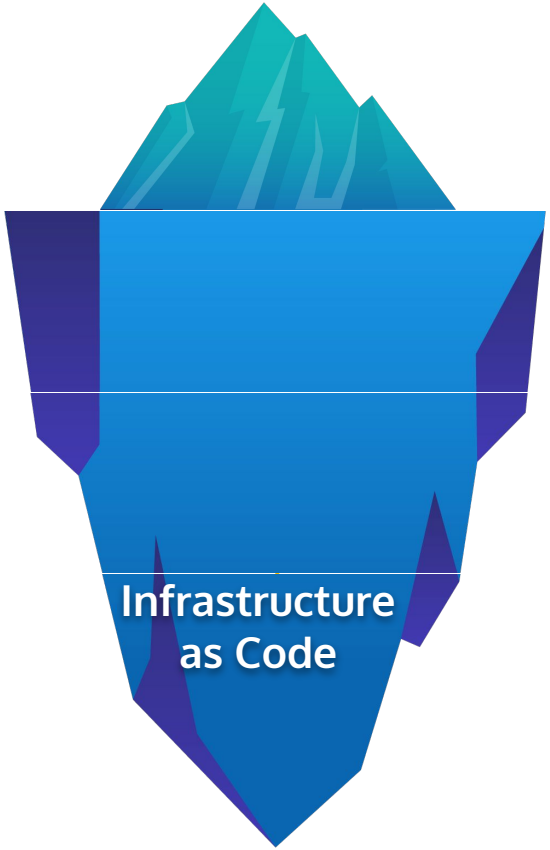
kubernetes

Amazon
S3

Firebase

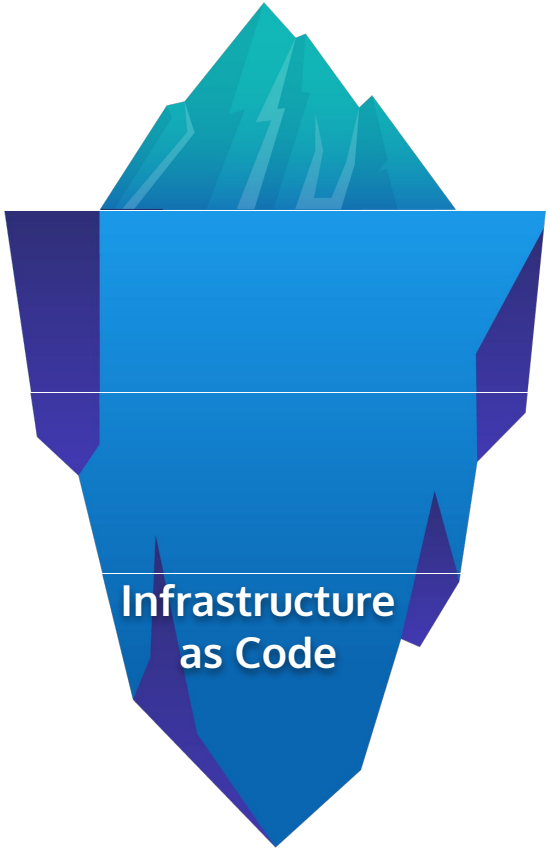


- #1 cloud vulnerability is misconfiguration [NSA]
- Network access, storage, servers - deployed as fast as code



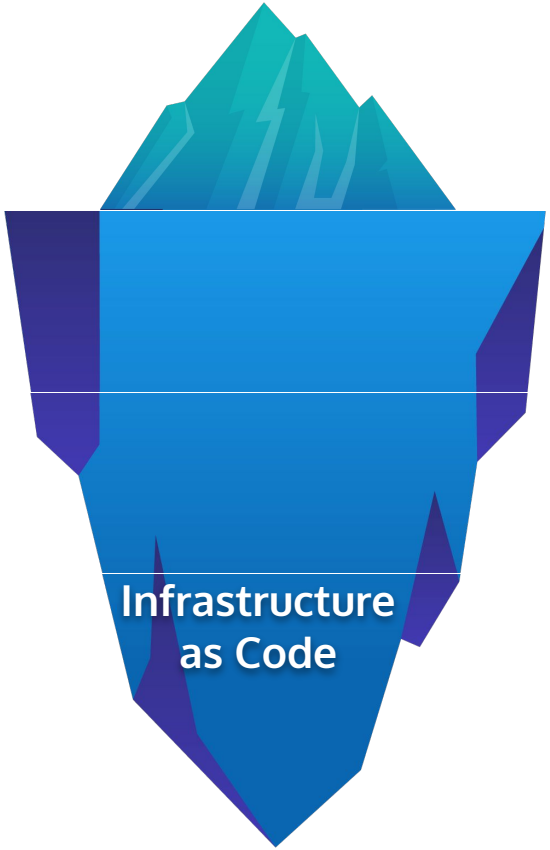

```
service cloud.firestore {
  match /databases/{database}/documents {
    match /{document=**}/
      allow read, write: if request.auth != null;
    }
  }
}
```

Firebase



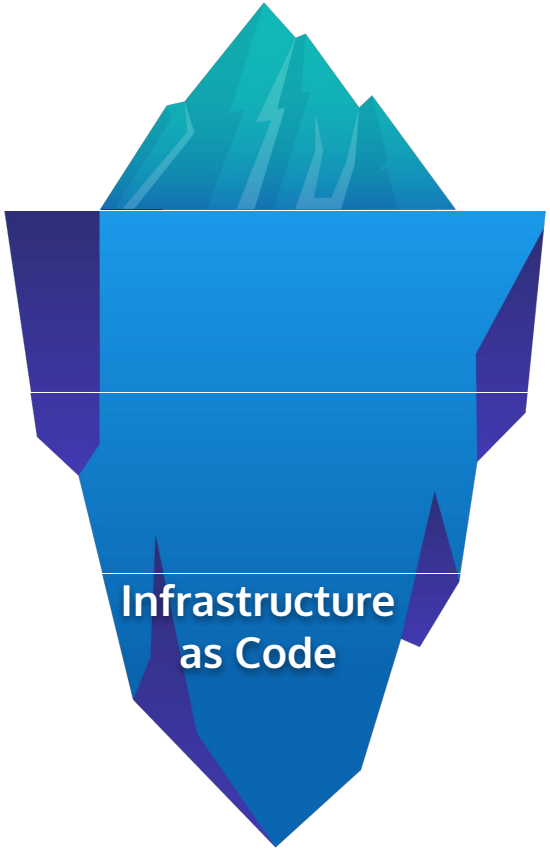

```
template:
  spec:
    containers:
      - name: goof
        image: goof:latest
        ports:
          - containerPort: 3001
          - containerPort: 9229
        env:
          - name: DOCKER
            value: "1"
```

kubernetes




```
template:
  spec:
    securityContext:
      runAsNonRoot: true
    containers:
      - name: goof
        image: goof:latest
        ports:
          - containerPort: 3001
          - containerPort: 9229
        env:
          - name: DOCKER
            value: "1"
```

kubernetes



Issues 8

Search issues…

0 H 2 M 6 L

Line #4

> Container is running without AppArmor profile L

Line #18

> Container is running with default set of capabilities M

Path: [DocId: 0] > input > spec > template > spec > containers[goof] > securityContext > capabilities > drop

> The issue is...
Default capabilities are not explicitly dropped

> The impact of this is...

> You can resolve this by...
Add ALL to securityContext.capabilities.drop list

Ignore

```yaml
---
apiVersion: apps/v1
kind: Deployment
metadata:
  name: goof
spec:
  replicas: 1
  strategy: {}
  selector:
    matchLabels:
      app: goof
  template:
    metadata:
      labels:
        app: goof
    spec:
      containers:
      - image: snykschmidtty/goof-kubernetes
        name: goof
        ports:
        - containerPort: 3001
        - containerPort: 9229
        resources: {}
        env:
          - name: "DOCKER"
            value: "1"
      restartPolicy: Always
```

Takeaways

Takeaways

Connect your source-code repositories to continuously scan them

Takeaways

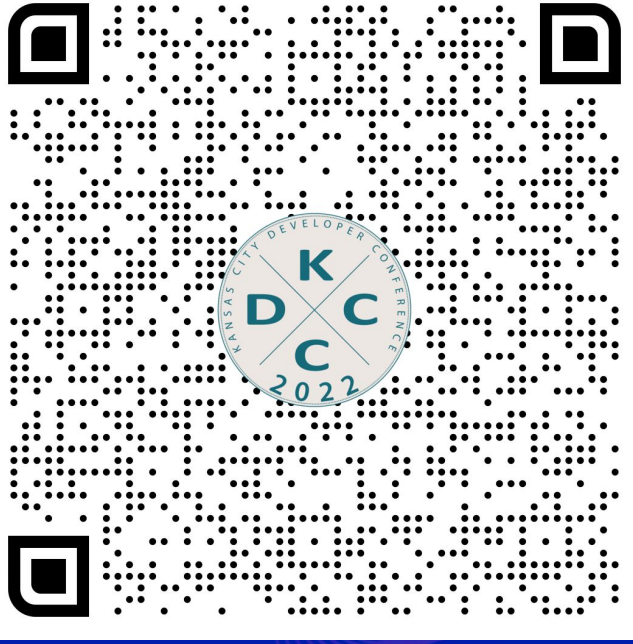
Connect your container image registries to always scan them too

Takeaways

Prefer minimal base images,
and act fast with base image recommendations

Takeaways

Your infrastructure is just as vulnerable, take measures to monitor and fix it



Stay safe in your journey to

Cloud Native Application Security :-)

https://snyk.io/blog

https://github.com/snyk-labs