



# 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

# What is the future of open source software security?

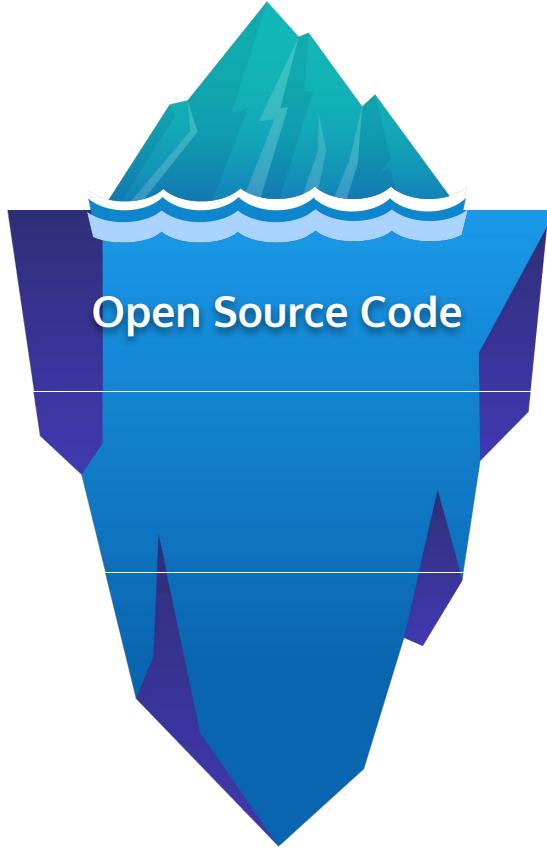


```
exports.admin = function (req, res, next) {  
  
  User.find(  
    {  
      username: req.body.username,  
      password: req.body.password  
    },  
    function (err, users) {}  
  );  
};
```



```
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



Red Yellow Green

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

    return s.replace(QUOT,'"').replace(SQUOTE, "'");
  }

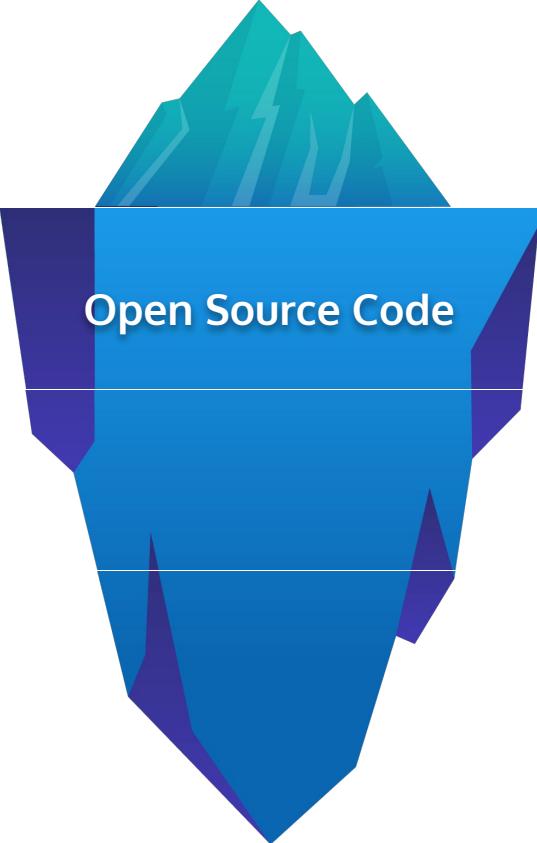
  return s;
};
```

HIGH SEVERITY

644

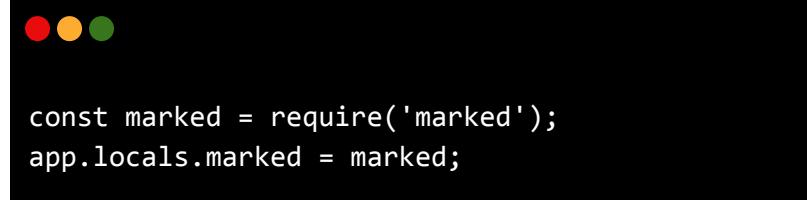
🛡️ Code Injection

Vulnerable module: [dustjs-linkedin](#)  
Introduced through: [dustjs-linkedin@2.5.0](#)  
Exploit maturity: No known exploit  
Fixed in: 2.6.0

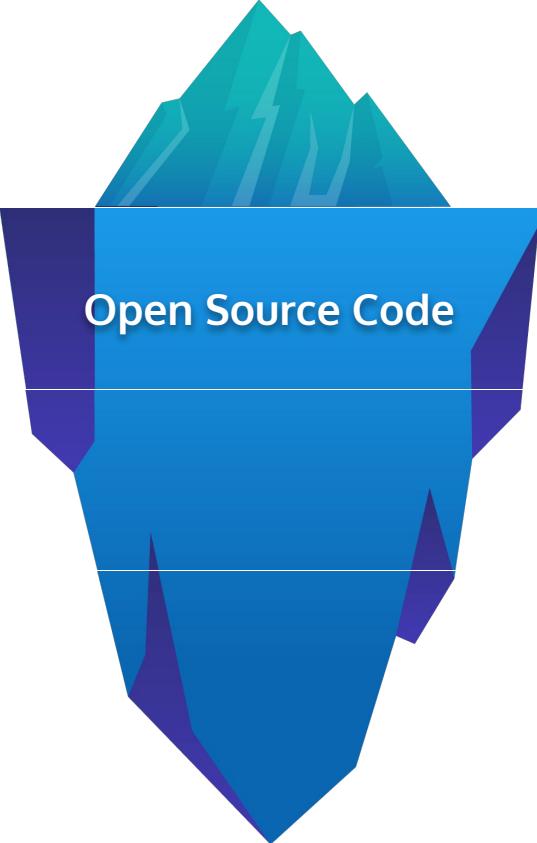


Open Source Code

Your Code



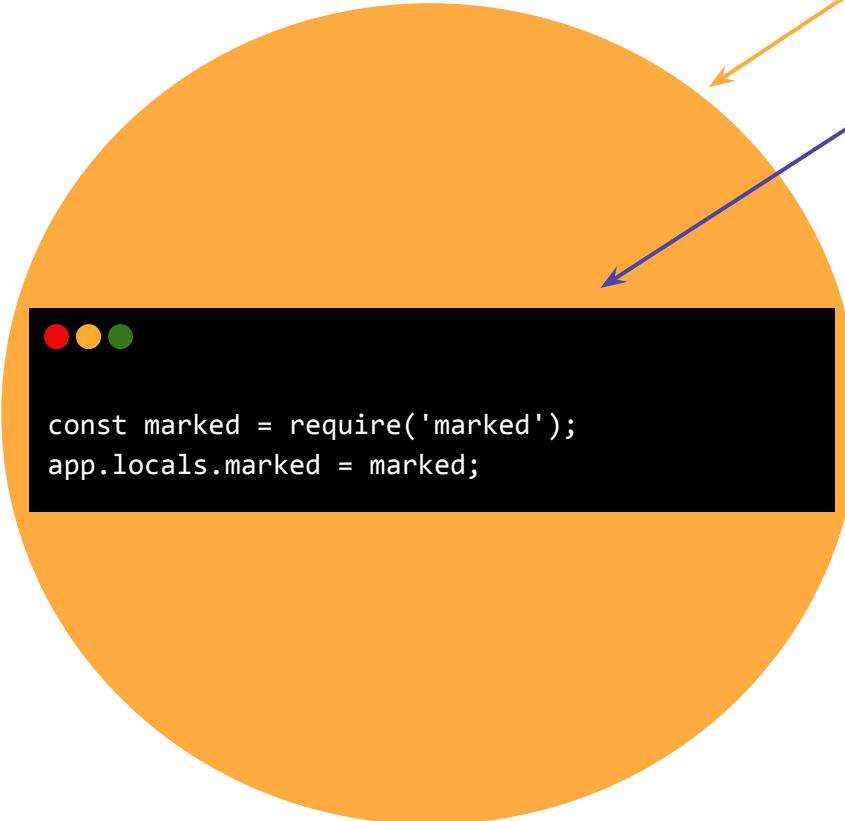
```
const marked = require('marked');
app.locals.marked = marked;
```



**Open Source Code**

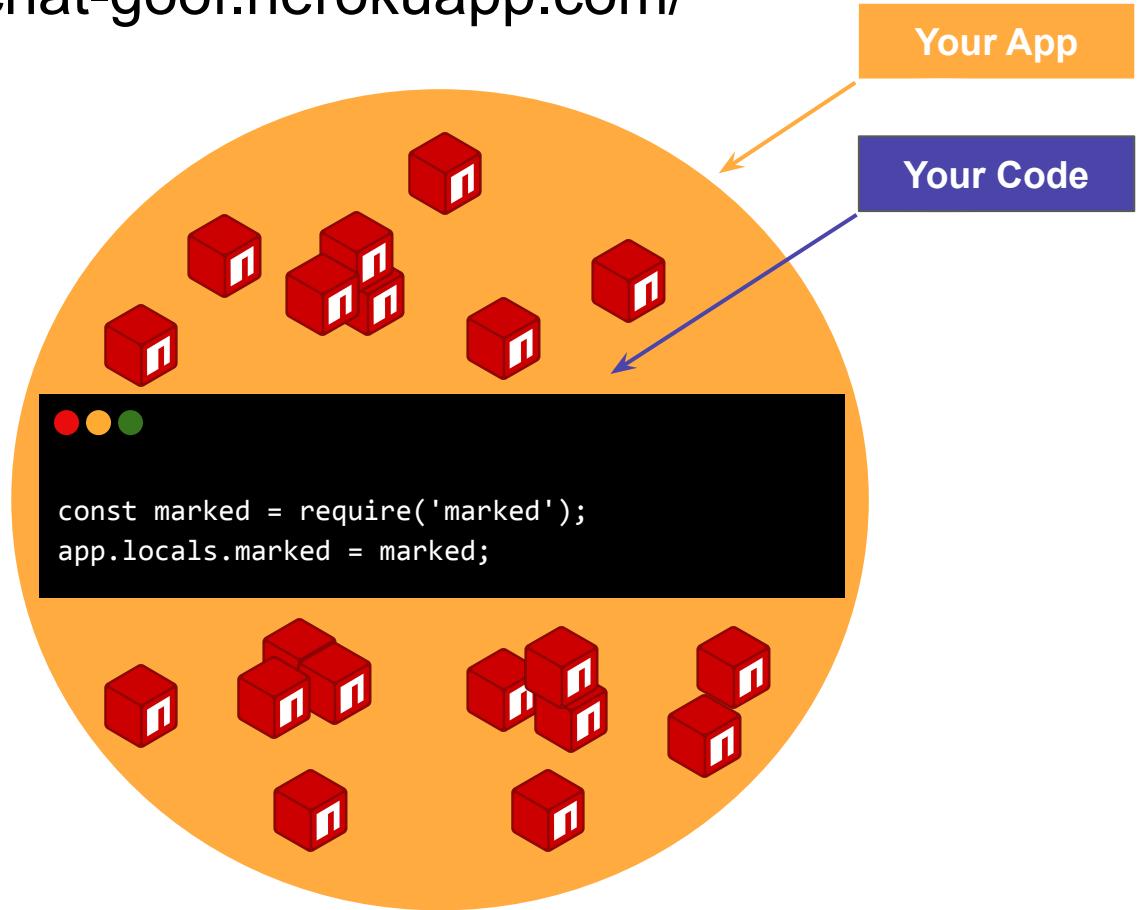
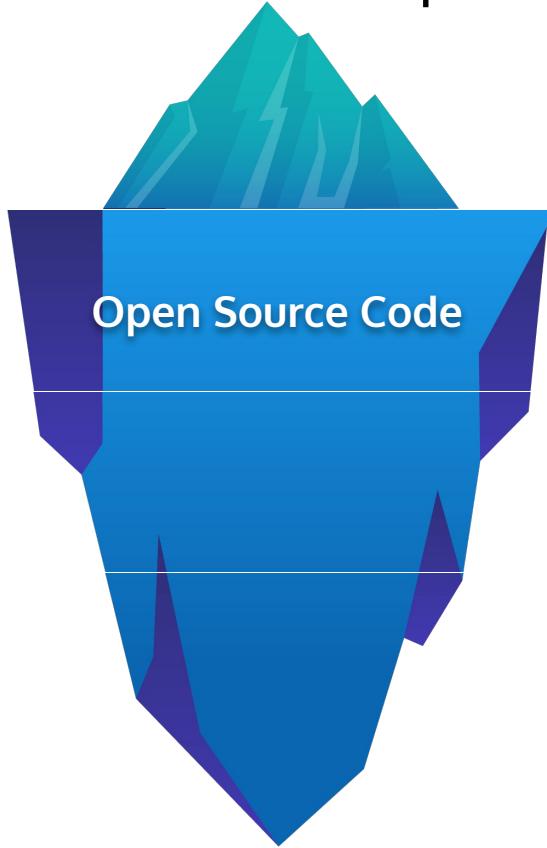
Your App

Your Code



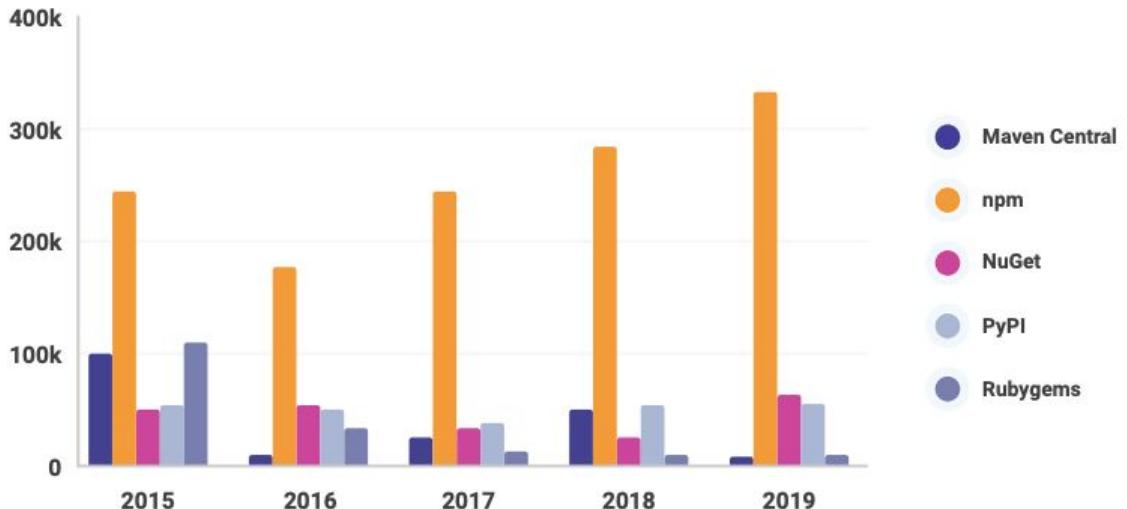
```
const marked = require('marked');
app.locals.marked = marked;
```

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

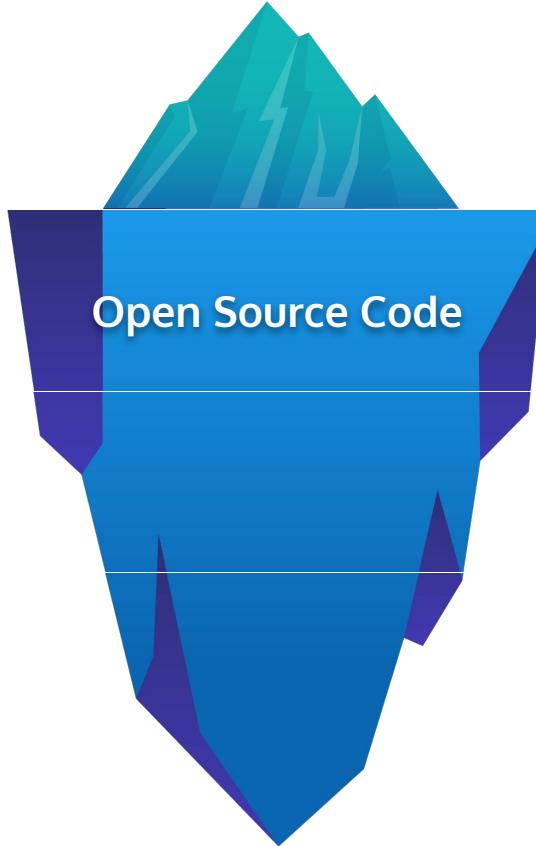




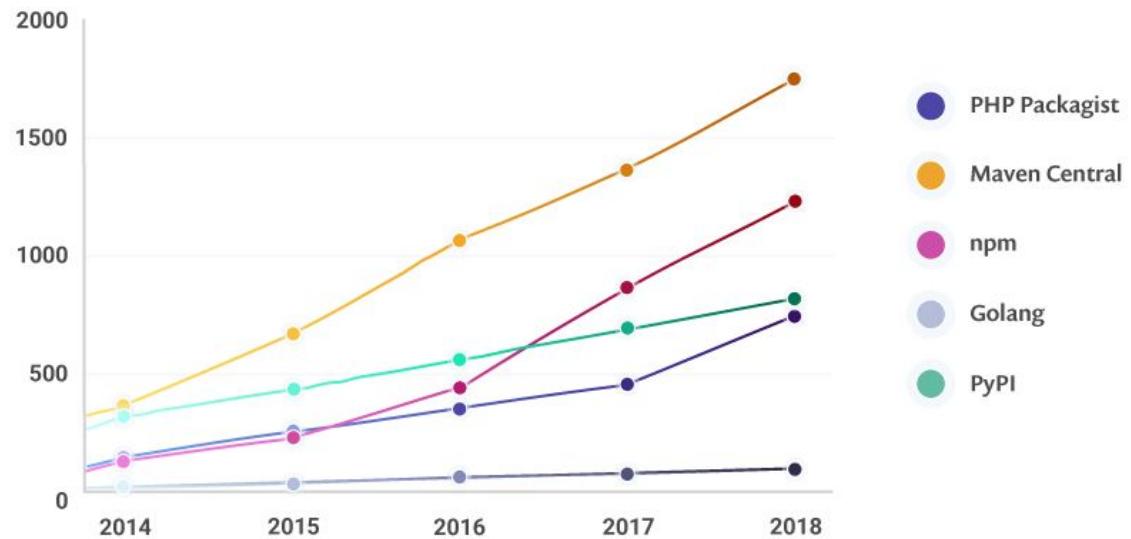
### New packages created by ecosystem per year



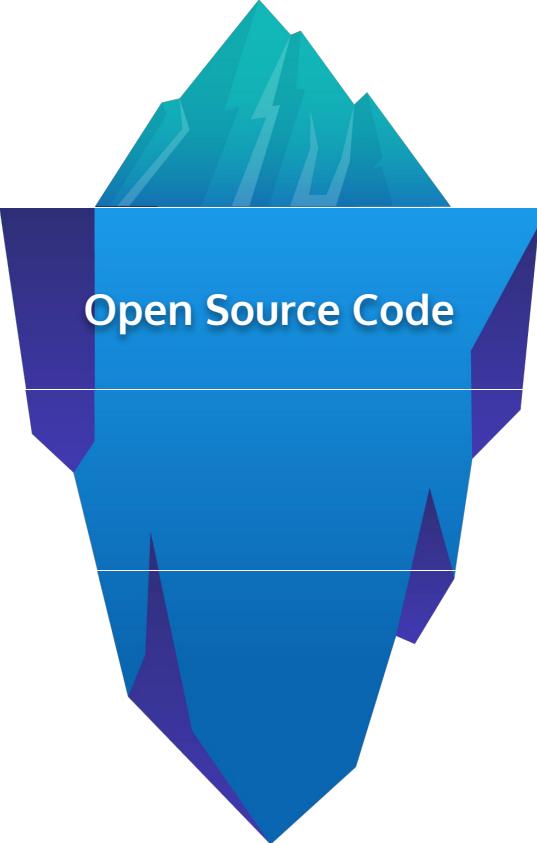
source: <https://snyk.io/open-source-security>



## New vulnerabilities each year by ecosystem

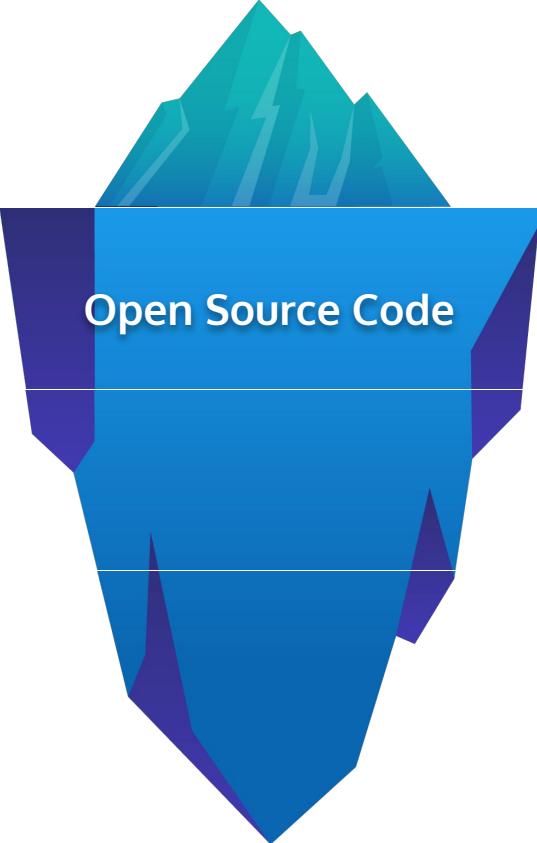


source: <https://snyk.io/open-source-security>



Open Source Code

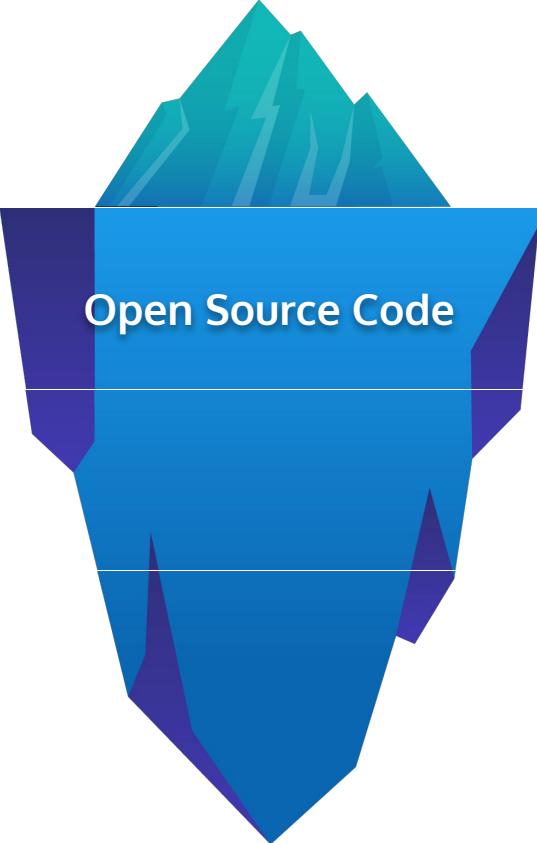
# Open-Source Supply Chain Security



Open Source Code

# Open-Source Supply Chain Security





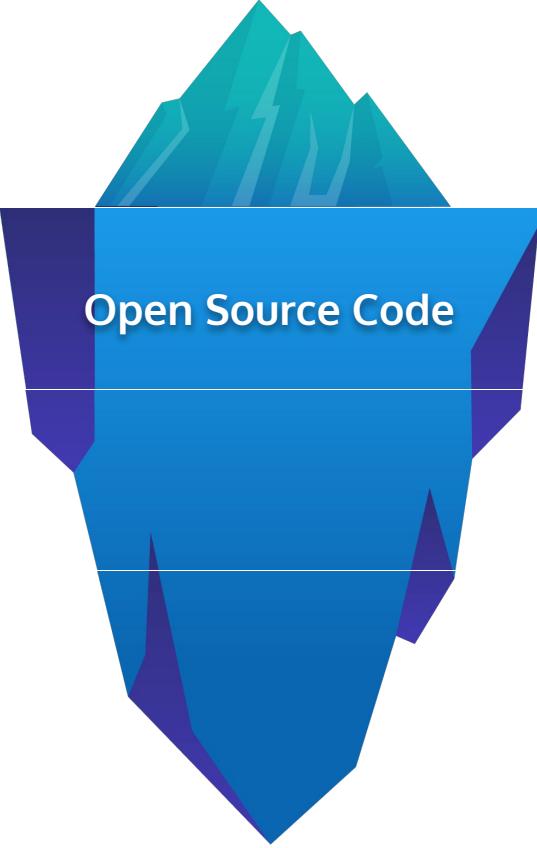
Open Source Code

# Open-Source Supply Chain Security



electron-native-notify

2019



Open Source Code

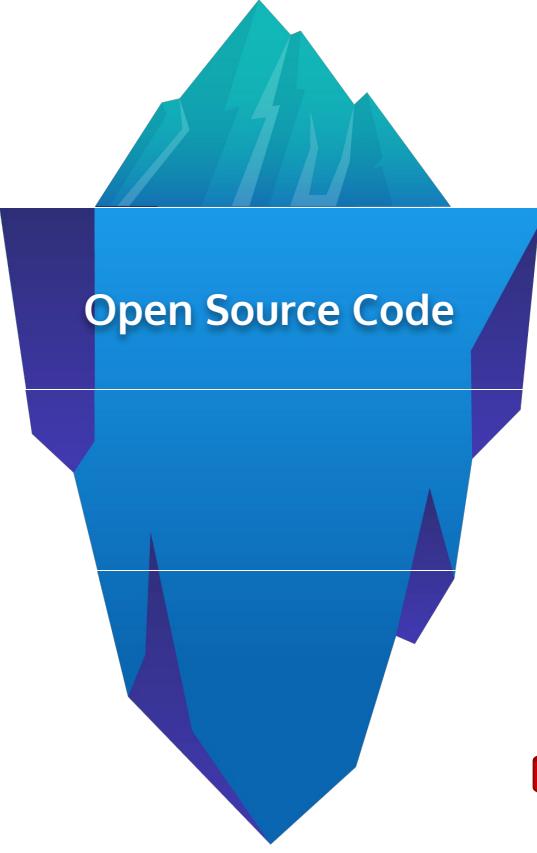
# Open-Source Supply Chain Security



electron-native-notify

2019

- **6 March 2019:** Non-malicious electron-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.
  - **16 Apr - 11 May 2019:** The Agama Wallet is rebuilt and published, using the most recent version of the electron-native-notify library, which at the time is 1.2.0
  - **5 June 2019:** npm and Komodo publicly announce the security flaws to their users.
- 
- **8 March 2019:** 9 minor releases later, electron-native-notify v1.1.5 is published to npm
  - **23 Mar 2019:** Malicious version of electron-native-notify package published to npm at version 1.1.6
  - **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.



Open Source Code

# Open-Source Supply Chain Security

2020



urijs@1.18.12

Medium severity,  
Improper Input Validation

2020



frappe-charts

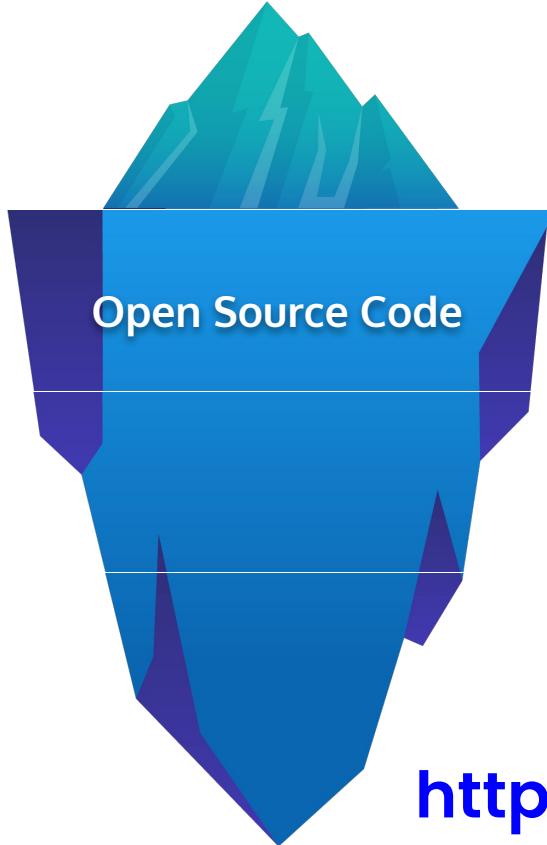
Medium severity,  
Cross-site Scripting (XSS)

2021



ejs@\*

High severity,  
Arbitrary Code Injection



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

# Open Source Code

snyk Advisor  Search packages 

Open Source Basics  Ecosystem Insights  Code Securely  About Us 

**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

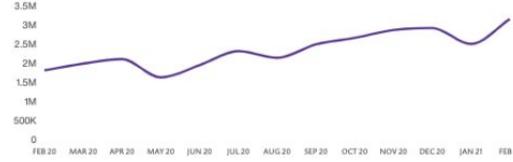
[date-fns 87 / 100](#) > [torque 42 / 100](#) > [movement 36 / 100](#) >

**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 

**Popularity**   
WEEKLY DOWNLOADS (17,789,231)



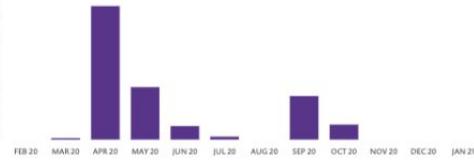
DEPENDENTS: 46.35K GITHUB STARS: 45.38K FORKS: 6.84K CONTRIBUTORS: 420

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**   
COMMIT FREQUENCY



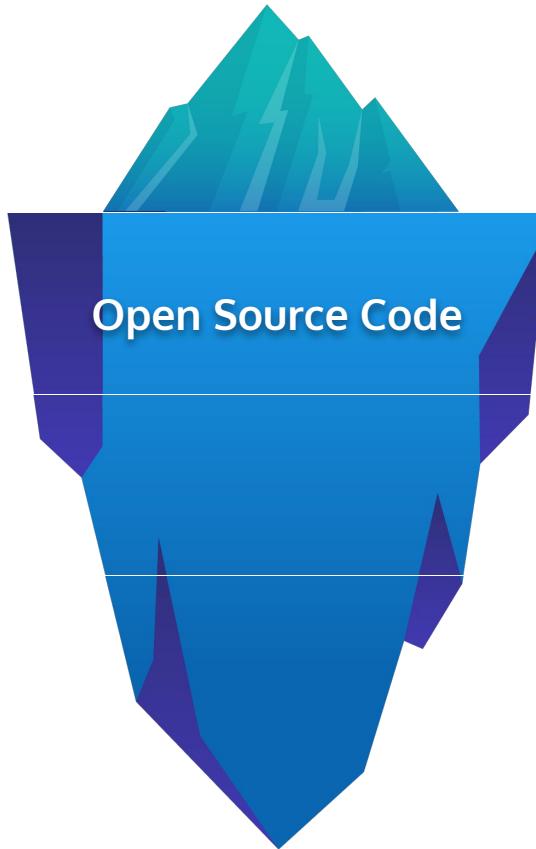
OPEN ISSUES	MERGED PR	OPEN PR	LAST COMMIT
87	707	31	3 months ago

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.

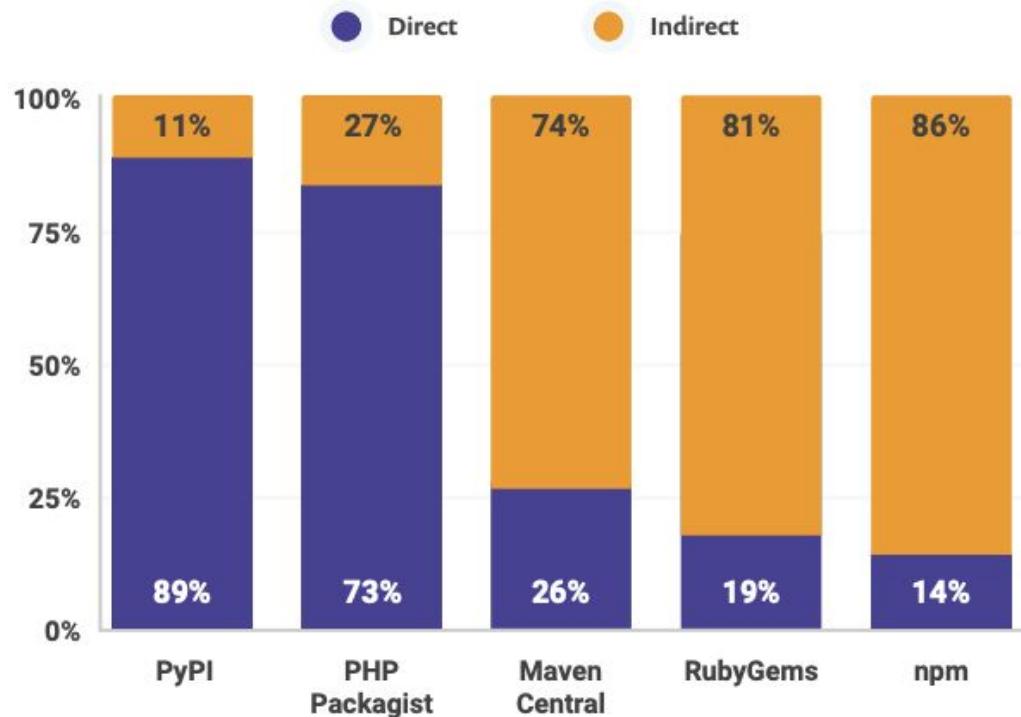
We found that moment demonstrates a positive version release cadence with at least one new version released in the past 12 months.

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>



## Vulnerabilities from direct versus indirect dependencies



# Open Source Code

[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

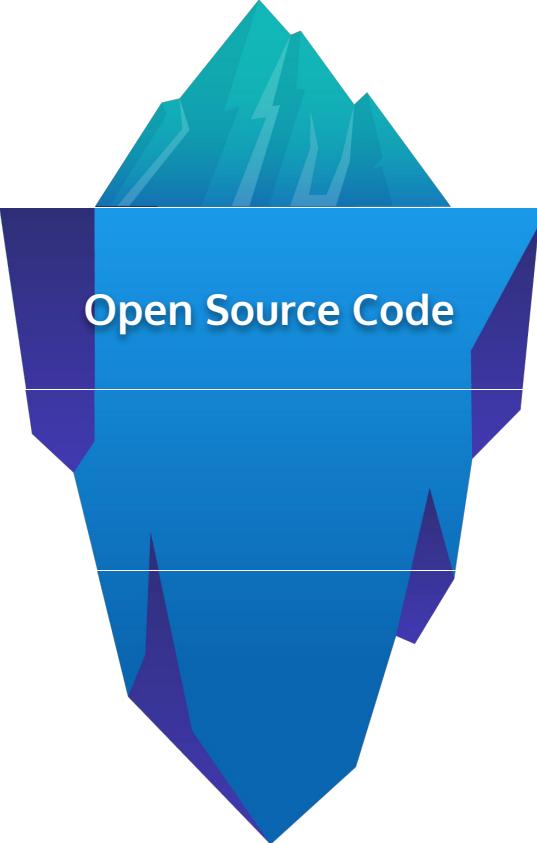
# Open Source Code

The screenshot shows the Snyk web application interface. At the top, there are three colored dots (red, yellow, green) followed by the URL <https://app.snyk.io>. The header includes the Snyk logo, the text "Team Dagobah", and a user dropdown for "Liran Tal". Below the header, the navigation bar has tabs for "Dashboard", "Reports", "Projects" (which is selected), "Integrations", and "Settings".

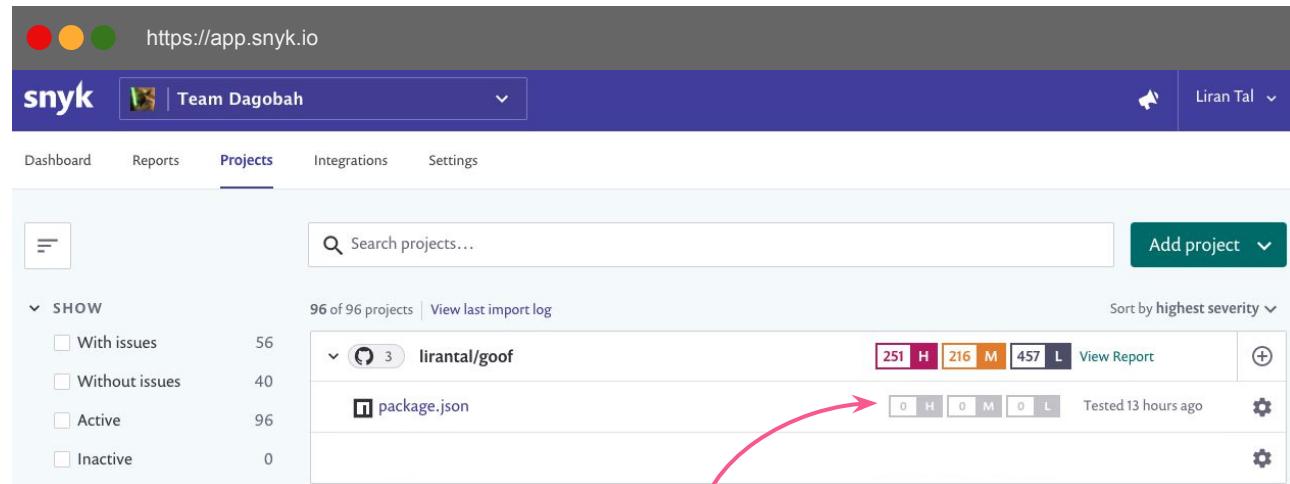
The main content area displays a list of projects. A search bar at the top right says "Search projects...". A button on the right says "Add project". Below the search bar, it says "96 of 96 projects | View last import log" and "Sort by highest severity".

A sidebar on the left titled "SHOW" contains filters: "With issues" (56), "Without issues" (40), "Active" (96), and "Inactive" (0). A red arrow points from the "Active" filter to the "package.json" entry in the project list.

The project list shows one item: "lirantal/goof" with a "package.json" file. It displays severity counts: 251 High (purple), 216 Medium (orange), and 457 Low (blue). It also shows "Tested 13 hours ago" and two gear icons for configuration.



Open Source Code



The screenshot shows the Snyk application interface. At the top, there are three colored dots (red, yellow, green) followed by the URL <https://app.snyk.io>. The header includes the Snyk logo, a user icon labeled "Team Dagobah", a dropdown menu, and a notification bell with the name "Liran Tal". Below the header, there are navigation tabs: Dashboard, Reports, Projects (which is selected), Integrations, and Settings. A search bar with the placeholder "Search projects..." is positioned above a list of projects. The list shows 96 of 96 projects, with a link to "View last import log" and a "Sort by highest severity" dropdown. The first project listed is "lirantal/goof" with a "package.json" file. The details for this project show 251 High (H) vulnerabilities, 216 Medium (M) vulnerabilities, and 457 Low (L) vulnerabilities, with a "View Report" button. A red curved arrow points from the "Open Source Code" text on the left to the "package.json" section of the Snyk interface.

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

lirantal/goof

package.json

251 H 216 M 457 L View Report

0 H 0 M 0 L Tested 13 hours ago

# App repository continuously scanned

# Open Source Code

https://app.snyk.io

snyk | Team Dagobah

Liran Tal

Dashboard Reports Projects Integrations Settings

Search projects... Add project

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

SHOW

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

lirantal/goof

package.json

251 H 216 M 457 L View Report

0 H 0 M 0 L Tested 13 hours ago

???





Containers, FaaS & Static Sites

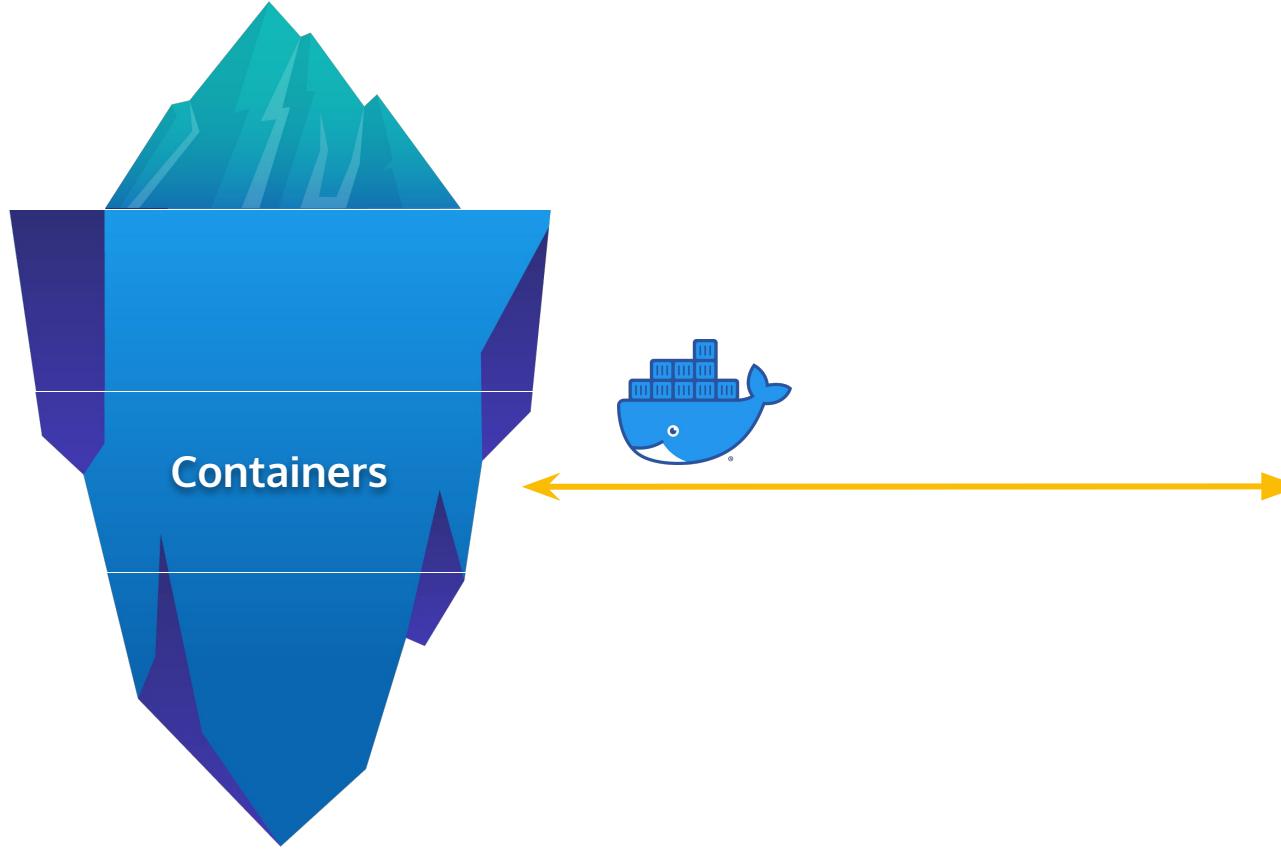


The Netlify logo, which consists of a teal diamond shape followed by the word "netlify" in a lowercase sans-serif font.

The Vercel logo, which features a black triangle pointing upwards positioned above the word "Vercel".



The AWS Lambda logo, which consists of an orange square with a white lambda symbol inside, with the text "AWS Lambda" written below it.





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

lirantal/goof

package.json

251 H 216 M 457 L View Report

0 H 0 M 0 L Tested 13 hours ago

???

The screenshot shows the Snyk web interface. At the top, there are three colored circles (red, yellow, green) followed by the URL 'https://app.snyk.io'. Below the header is a dark blue navigation bar with tabs: Dashboard, Reports, Projects (which is selected), Integrations, and Settings. On the right of the header is a user profile for 'Liran Tal' with a dropdown arrow. The main content area has a light gray background. On the left, there's a sidebar with a filter icon and a search bar containing 'Search projects...'. A button 'Add project' with a dropdown arrow is on the far right. The main list shows '96 of 96 projects' and a link to 'View last import log'. A 'Sort by highest severity' dropdown is also present. The first project listed is 'lirantal/goof' with a 'package.json' file. To the right of the project name are three colored boxes: purple for 'H' (High), orange for 'M' (Medium), and teal for 'L' (Low). Below these are buttons for 'View Report' and a gear icon. Further down, there are buttons for '0 H', '0 M', and '0 L' with a note 'Tested 13 hours ago'. A gear icon is also present here. A red arrow originates from three question marks ('???' in red) at the bottom left and points upwards towards the 'package.json' entry in the list. The entire interface is framed by a thin gray border.



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

Project	Dependencies	Issues	Severity	Tested	Action
lirantal/goof	package.json Dockerfile	251 H 216 M 457 L	View Report	13 hours ago	
lirantal/goof	package.json Dockerfile	216 H 187 M 452 L	View Report	4 hours ago	

A red arrow points from a blue Docker whale icon at the bottom center up towards the "Dockerfile" entry in the Snyk dashboard results list.



```
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" ]
```

A screenshot of a terminal window showing a Dockerfile. The file starts with a `FROM node` instruction. It then runs two `RUN apt-get` commands to update the package list and install the `imagemagick` library. Next, it uses `COPY` to copy the current directory contents to `/usr/src/goof`, sets the `WORKDIR` to that location, runs `npm install`, and finally specifies the command to run as `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+deb9u11`  
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?



#### January 2021 Security Releases

by Michael Dawson, 2021-01-04

(Update 4-Jan-2021) Security releases available

Updates are now available for v10.x, v12.x, v14.x and v15.x Node.js release lines for the following issues.

In addition to the vulnerabilities listed below, these releases also include an update to npm in order to resolve an issue that was reported against npm by security scanners even though it was not vulnerable.

use-after-free in TLSWrap (High) (CVE-2020-8265)

# Digital transformation means rapid container adoption

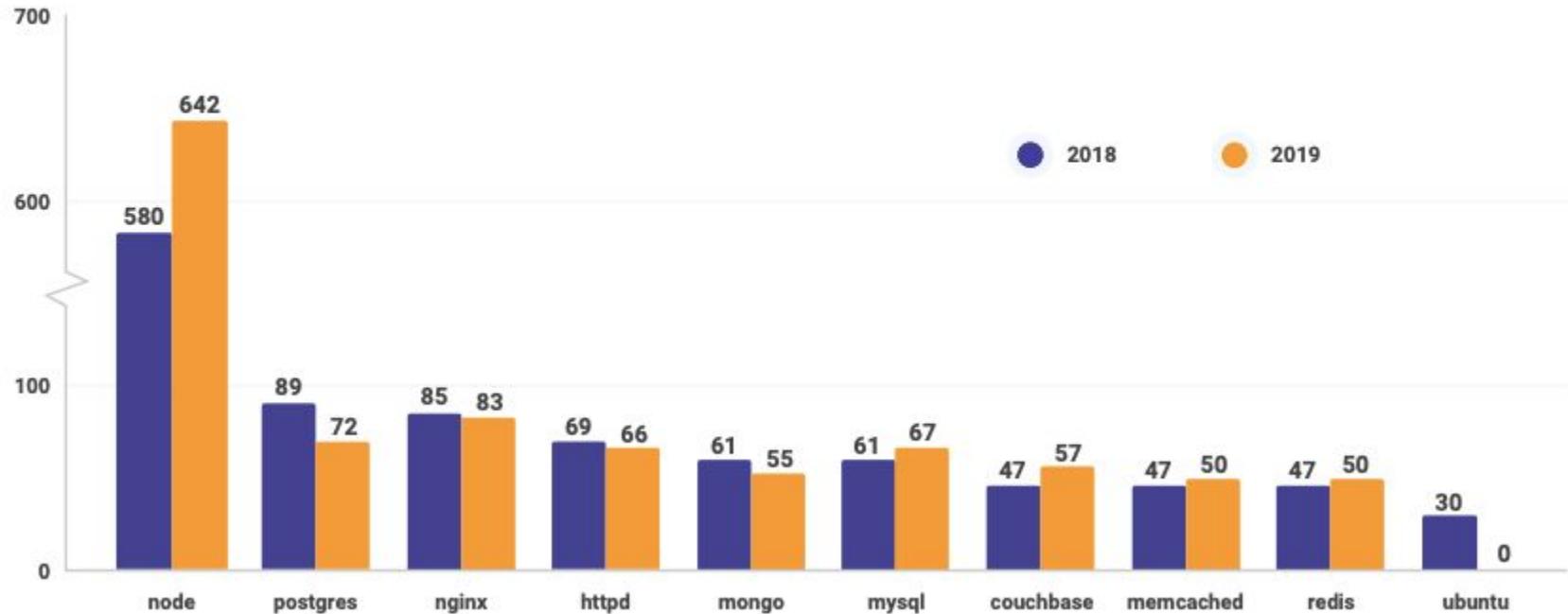
---

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;

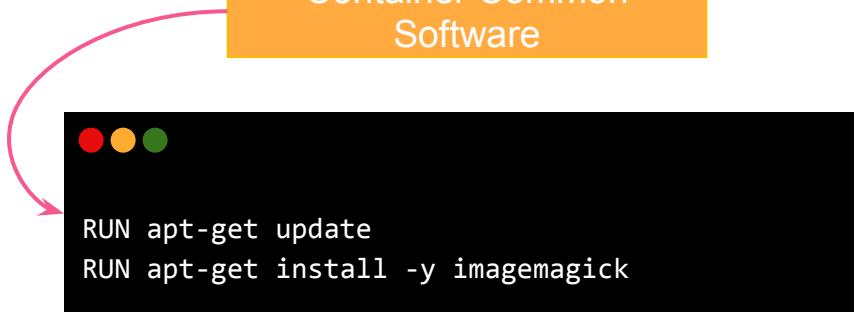
<div class="item">
  <a href="/edit/<%= todo._id %>">
    <%- marked(new String(todo.content)) %>
  </a>
</div>
```

# Let's hack a Node.js application!

we will exploit:

An Open Source Library

Container Common  
Software



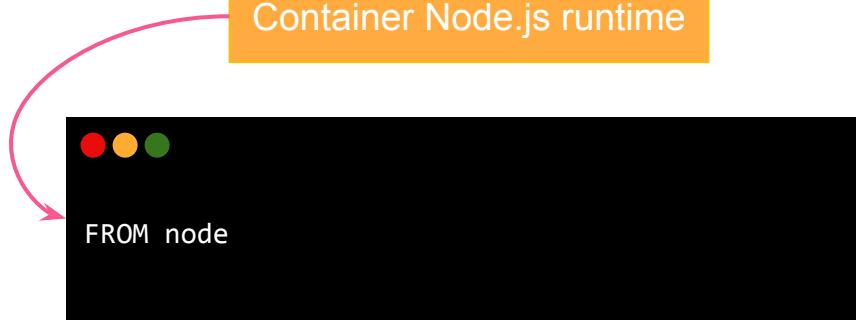
# Let's hack a Node.js application!

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... ?

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-Subuntu3.4 || 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`

Do your applications use this vulnerable package?

[Test your applications](#)

### Overview

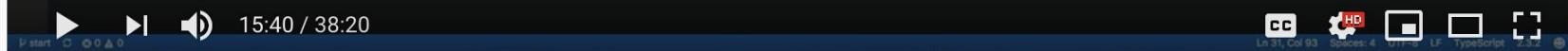
The (1) Ephemeral, (2) HTTPS, (3) MVG, (4) MSL, (5) TEXT, (6) SHOW, (7) WIN, and (8) PLT coders in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allow remote attackers to execute arbitrary code via shell metacharacters in a crafted image, aka "ImageTragick."

### References

- ADVISORY [🔗](#)
- BID [🔗](#)
- BUGTRAQ [🔗](#)
- BUGTRAQ [🔗](#)
- CERT-VN [🔗](#)
- CONFIRM [🔗](#)
- CONFIRM [🔗](#)
- CONFIRM [🔗](#)



```
14
15  exports.resizeImage = functions.storage.object().onChange(async event => {
16    const path = event.data.name;
17    const [imgType, uid, id] = path.split("/");
18
19    // we only want to resize newly uploaded images
20    if (imgType !== "upload") return;
21
22    // download the image locally
23    const tmpFilePath = `/tmp/${id}.jpg`;
24    const file = bucket.file(path);
25    await file.download({destination: tmpFilePath});
26
27    // Generate a thumbnail using ImageMagick.
28    await spawn('convert', [tmpFilePath, '-thumbnail', '900x900>', tmpFilePath]);
29
30    // upload the newly resized image to GCS
31    await bucket.upload(tmpFilePath, {destination: `resized/${uid}/${id}.jpg`, public: true});
32});
```



#io17 #GoogleI/O #GoogleI/O2017

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

18,358 views • May 17, 2017

18 220

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 > imagemagick/libmagickwand-dev@8:6.8.9.9-5+deb8u12
- **Introduced through:** lirantal/docker-goof:latest > imagemagick/libmagickcore-dev@8:6.8.9.9-5+deb8u12
- **Introduced through:** lirantal/docker-goof: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
Taken by:	Recurring
Image ID:	2a78ab879533
Runtime:	docker 19.03.2

Dependencies: 383

Hostname: Lirans-MBP

Image tag: 10.4.0

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

Snapshot taken by recurring test 5 hours ago.

Vulnerabilities: 862 via 7657 paths

Taken by: Recurring

Image ID: 2a78ab879533

Runtime: docker 19.03.2

Dependencies: 383

Hostname: Lirans-MBP

Image tag: 10.4.0

Imported by: Liran Tal liran@snyk.io

### Recommendations for base image upgrade

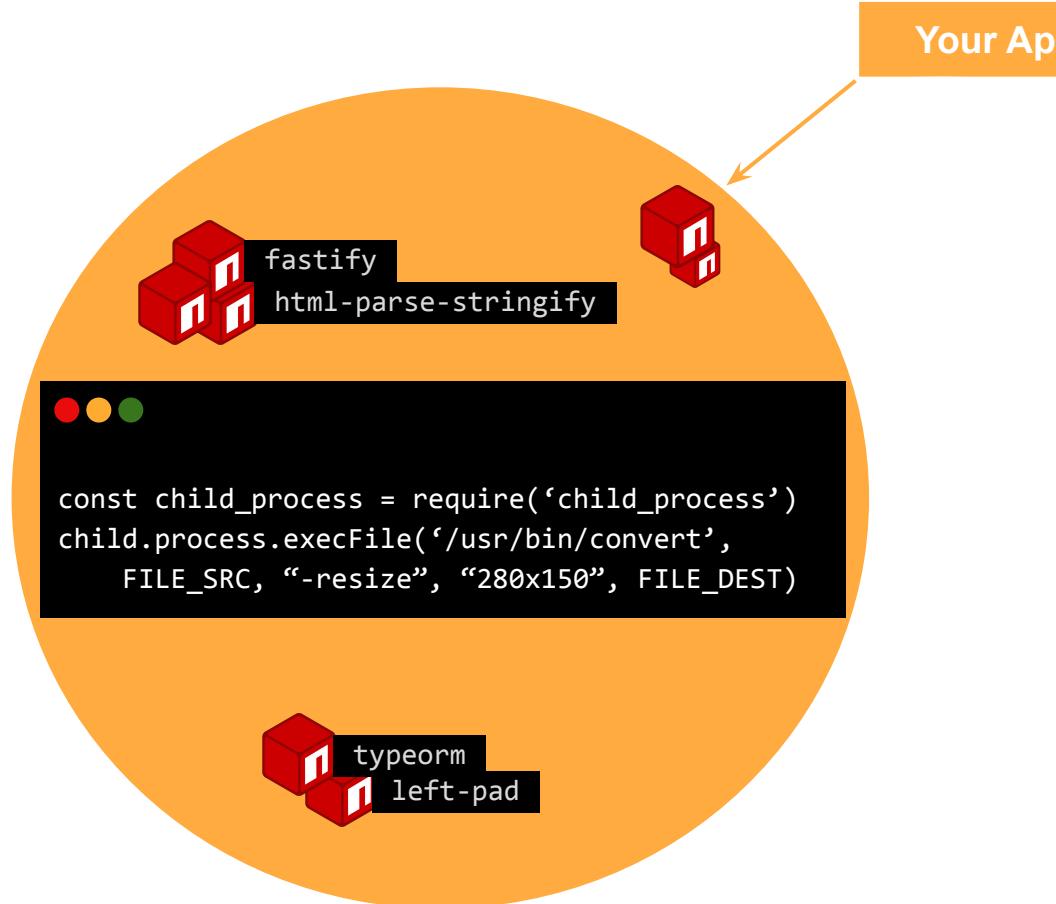
	BASE IMAGE	VULNERABILITIES	SEVERITY
Current image	node:10.4.0	862	390 high, 451 medium, 2
Minor upgrades	node:10.16.0	633	256 high, 356 medium, 2
Major upgrades	node:12.12.0	598	244 high, 339 medium, 1
Alternative upgrades	node:10.16.3-buster-slim	54	20 high, 26 medium, 8 low

Your Code



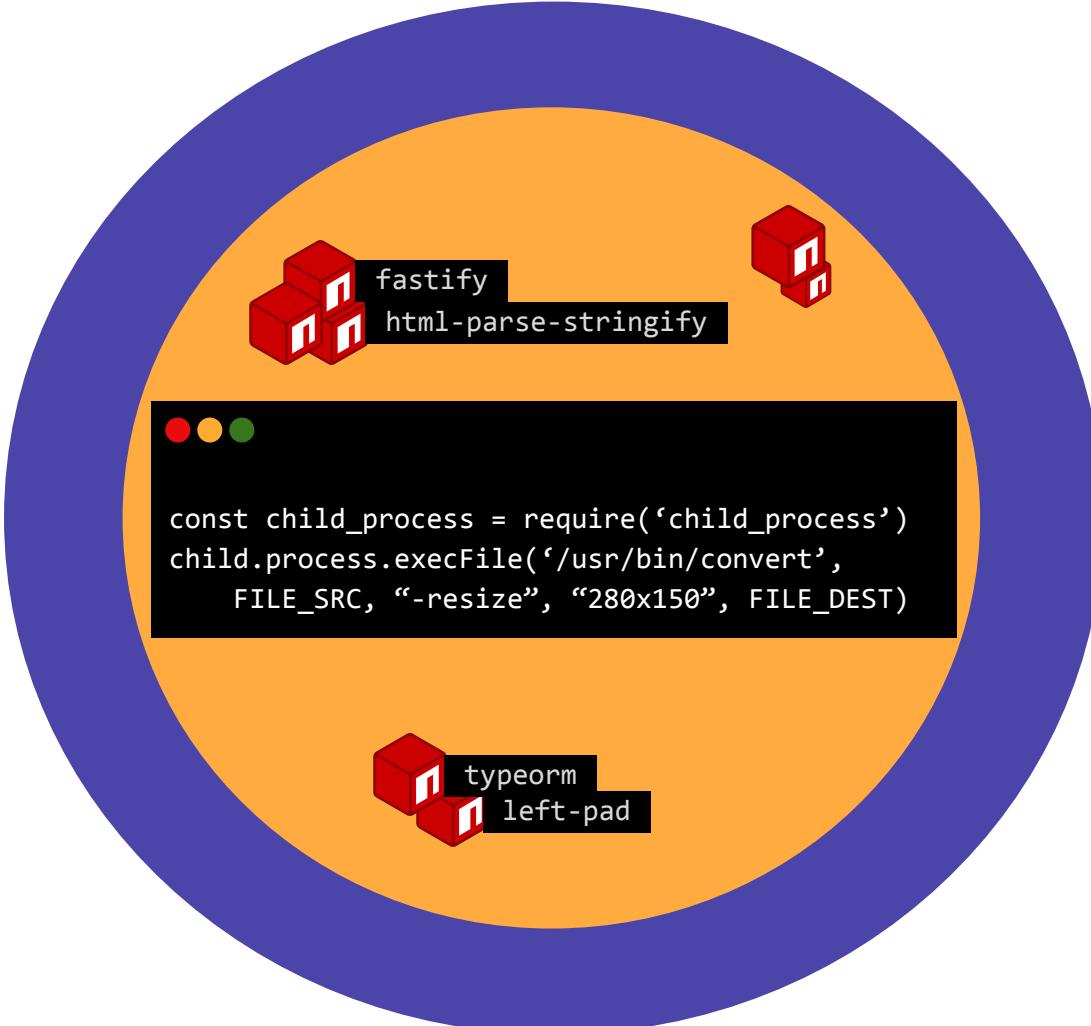
```
const child_process = require('child_process')
child_process.execFile('/usr/bin/convert',
    FILE_SRC, "-resize", "280x150", FILE_DEST)
```

Your App



## Your Container Deps & Runtime



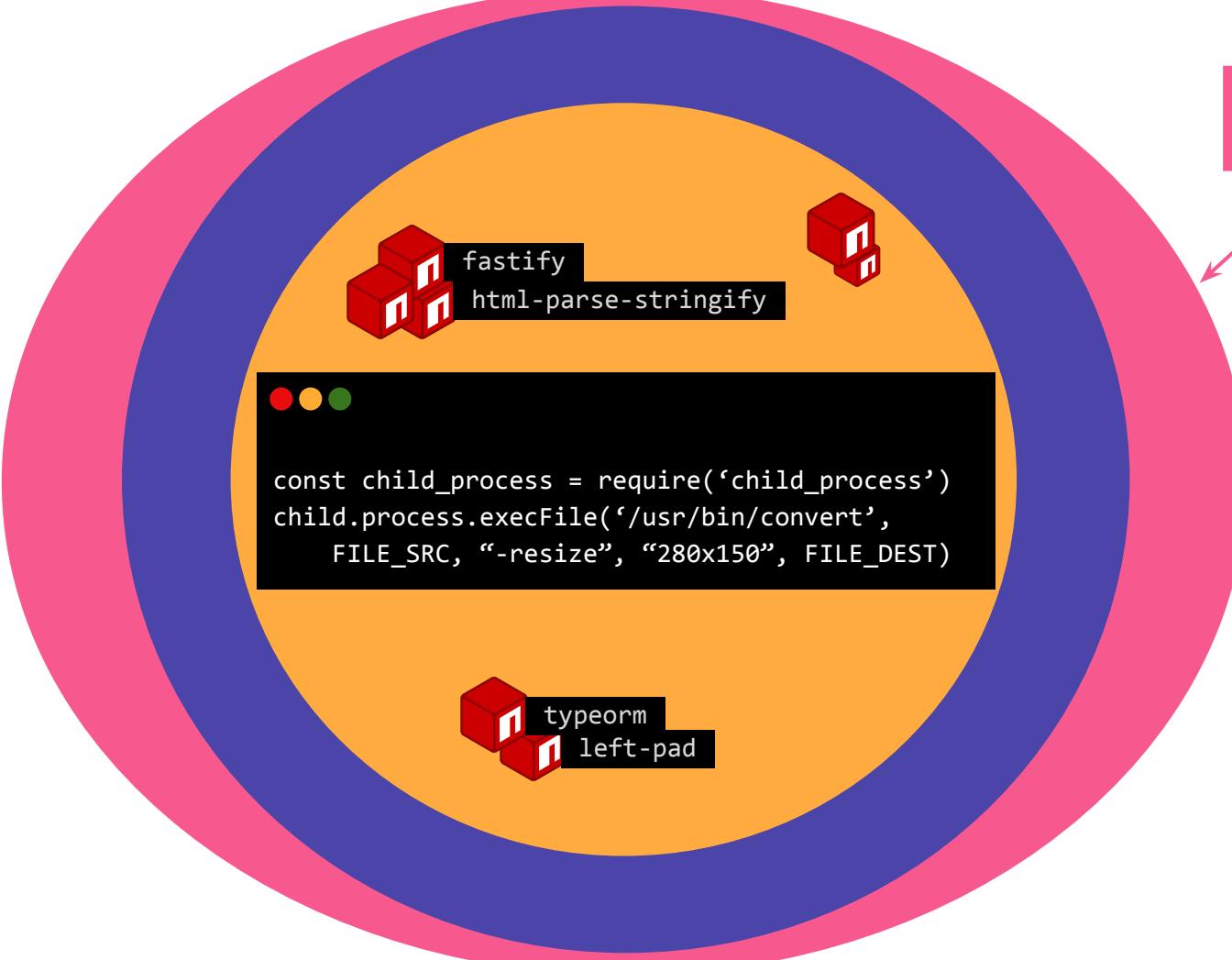


What else????

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

fastify  
html-parse-stringify

typeorm  
left-pad

```
const child_process = require('child_process')
child_process.execFile('/usr/bin/convert',
  FILE_SRC, "-resize", "280x150", FILE_DEST)
```

Infrastructure  
as Code

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



Infrastructure  
as Code

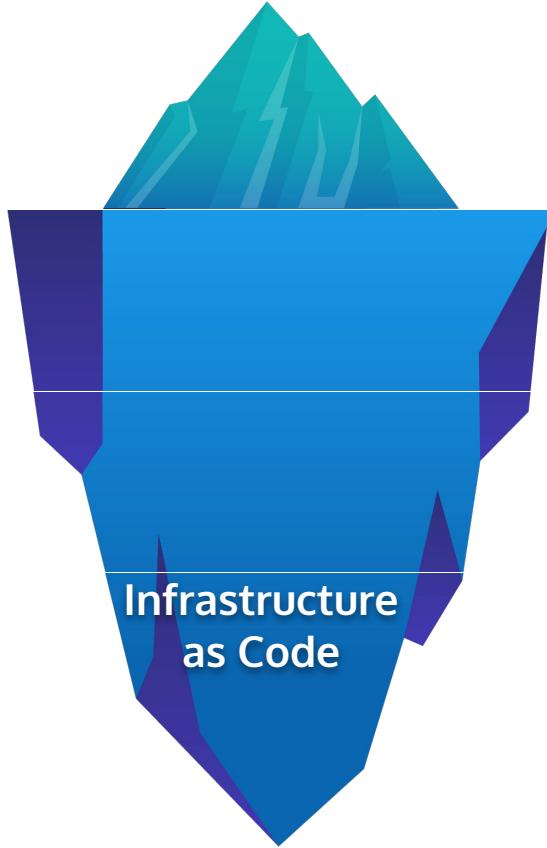


kubernetes



Firebase

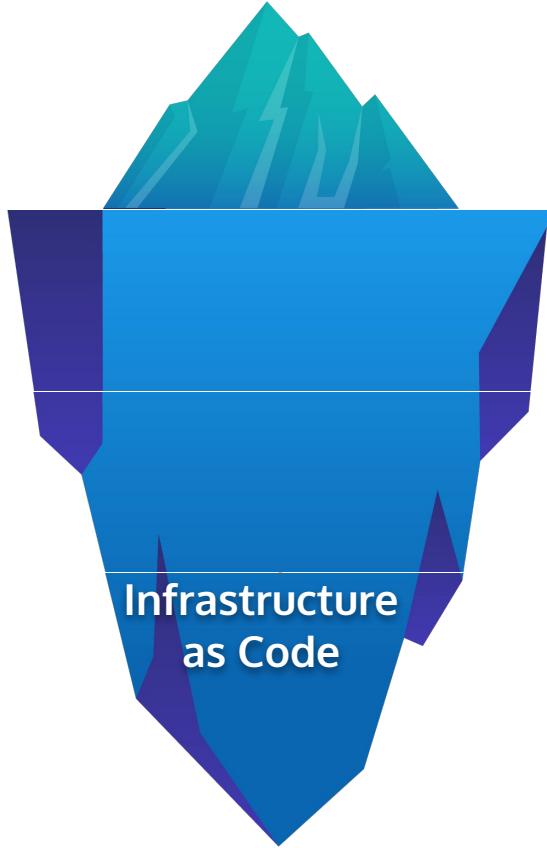




#1 cloud vulnerability is misconfiguration [NSA]

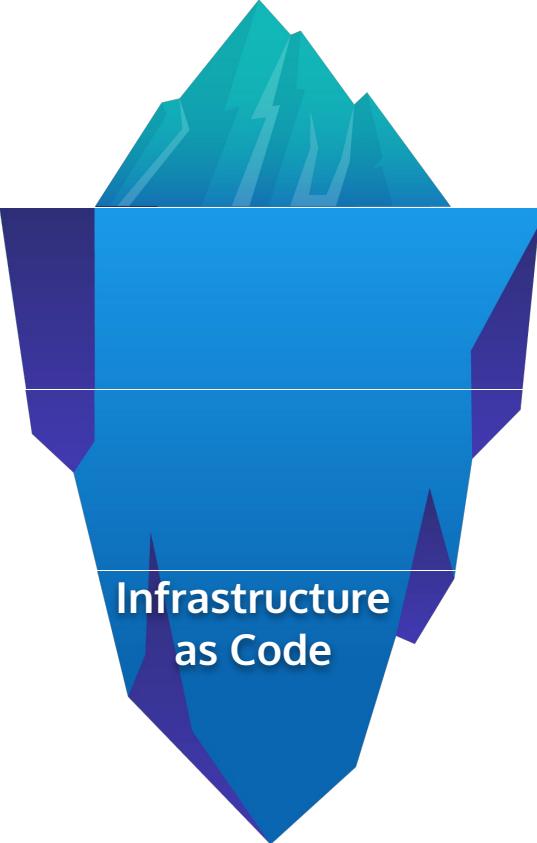


Network access, storage, servers - deployed as fast as code

A screenshot of a Mac OS X terminal window. The title bar shows three colored window control buttons (red, yellow, green). The terminal itself contains the following text:

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

The lines "match /{document=\*\*}/" and "allow read, write: if request.auth != null;" are highlighted in orange.

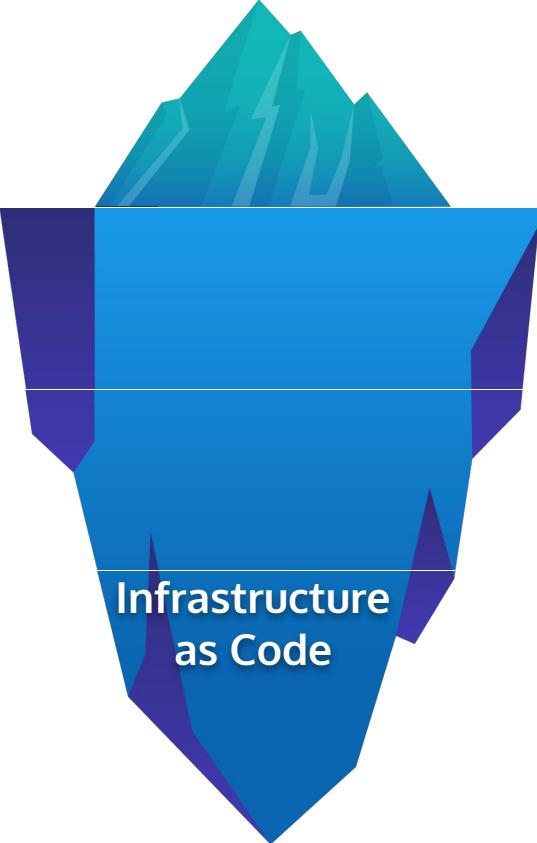


Infrastructure  
as Code

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



kubernetes

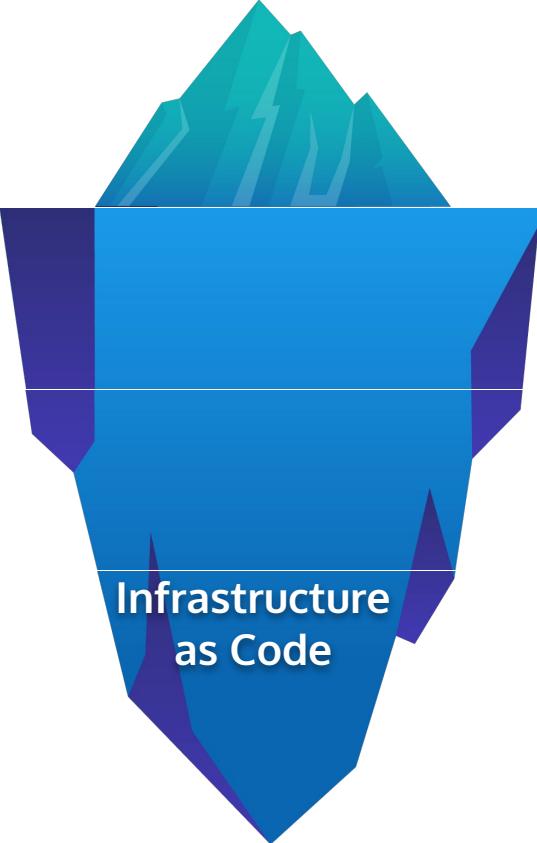


Infrastructure  
as Code

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



kubernetes



# Infrastructure as Code

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

```
1 ---  
2   apiVersion: apps/v1  
3   kind: Deployment  
4   metadata:  
5     name: goof  
6   spec:  
7     replicas: 1  
8     strategy: {}  
9     selector:  
10    matchLabels:  
11      app: goof  
12    template:  
13      metadata:  
14        labels:  
15          app: goof  
16      spec:  
17        containers:  
18          - image: snykschmidty/goof-kubernetes  
19            name: goof  
20            ports:  
21              - containerPort: 3001  
22              - containerPort: 9229  
23            resources: {}  
24            env:  
25              - name: "DOCKER"  
26                value: "1"  
27            restartPolicy: Always
```

# Takeaways

# Takeaways

Connect your source-code repositories to continuously scan them

# Takeaways

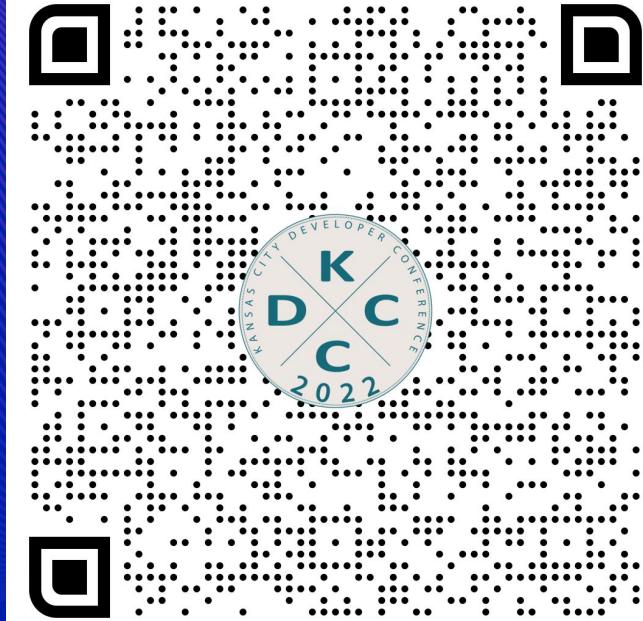
Connect your container image registries to  
always scan them too

# 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>