

# npm provenance

OWASP Oslo

Erlend Oftedal

# Open source component supply chain

- Which code went into it? Compiled?
- How was it built?
- Where was it built?
- (who built it? is security a focus? quality? etc. etc.)

express DT

4.18.2 • Public • Published 7 months ago

 [Readme](#)

 [Code](#) Beta

 [31 Dependencies](#)

 [71,885 Dependents](#)

 [270 Versions](#)

# express

Fast, unopinionated, minimalist web framework for **Node.js**.

npm v4.18.2 install size 1.89 MB downloads 115.3M/month

```
const express = require('express')
const app = express()

app.get('/', function (req, res) {
  res.send('Hello World')
})

app.listen(3000)
```

## Installation

This is a **Node.js** module available through the **npm registry**.

Before installing, **download and install Node.js**. Node.js 0.10 or higher is required.

### Install

```
> npm i express
```

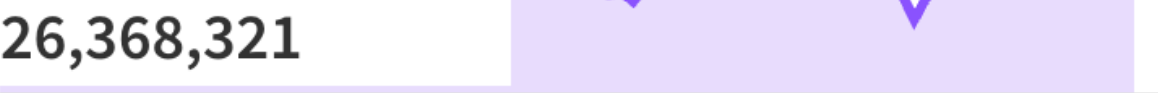
### Repository

 [github.com/expressjs/express](https://github.com/expressjs/express)

### Homepage

 [expressjs.com/](https://expressjs.com/)

### Weekly Downloads



Version	License
4.18.2	MIT
Unpacked Size	Total Files
214 kB	16
Issues	Pull Requests
112	54

Last publish  
7 months ago

Pull requests

Issues

Codespaces

Marketplace

Explore

expressjs / express

Public

Watch 1.7k

Fork 10.5k

Star 60.8k

<> Code

Issues 112

Pull requests 54

Discussions

Actions

Wiki

Security

Insights

4.18.2

8 branches

286 tags

Go to file

<> Code

dougwilson

4.18.2

✓

8368dc1 on Oct 8, 2022

🕒

5,752 commits

<div>📁</div> .github/workflows	build: Node.js@18.10	7 months ago
<div>📁</div> benchmarks	bench: remove unused parameter	last year
<div>📁</div> examples	examples: remove unused function arguments in params	last year
<div>📁</div> lib	Fix regression routing a large stack in a single route	last year
<div>📁</div> test	build: Node.js@18.10	7 months ago
<div>📄</div> .editorconfig	build: Add .editorconfig	6 years ago
<div>📄</div> .eslintignore	lint: add eslint rules that cover editorconfig	6 years ago
<div>📄</div> .eslintrc.yml	build: eslint@4.19.1	2 years ago
<div>📄</div> .gitignore	build: use nyc for test coverage	last year
<div>📄</div> Charter.md	docs: fix typo in casing of HTTP	last year
<div>📄</div> Code-Of-Conduct.md	docs: add Code of Conduct	3 years ago
<div>📄</div> Collaborator-Guide.md	docs: fix typos in Collaborator Guide	3 years ago
<div>📄</div> Contributing.md	docs: fix Code of Conduct link in Contributing	3 years ago
<div>📄</div> History.md	4.18.2	7 months ago
<div>📄</div> LICENSE	Merge tag '3.20.0'	8 years ago
<div>📄</div> Readme-Guide.md	docs: add guide for writing readmes	7 years ago

About

Fast, unopinionated, minimalist web framework for node.

🔗

expressjs.com

nodejs

javascript

express

server

📖

Readme

📄

MIT license

📄

Code of conduct

📄

Security policy

☆

60.8k stars

👁

1.7k watching

🔗

10.5k forks

Report repository

Releases

147

📦

4.18.2 Latest

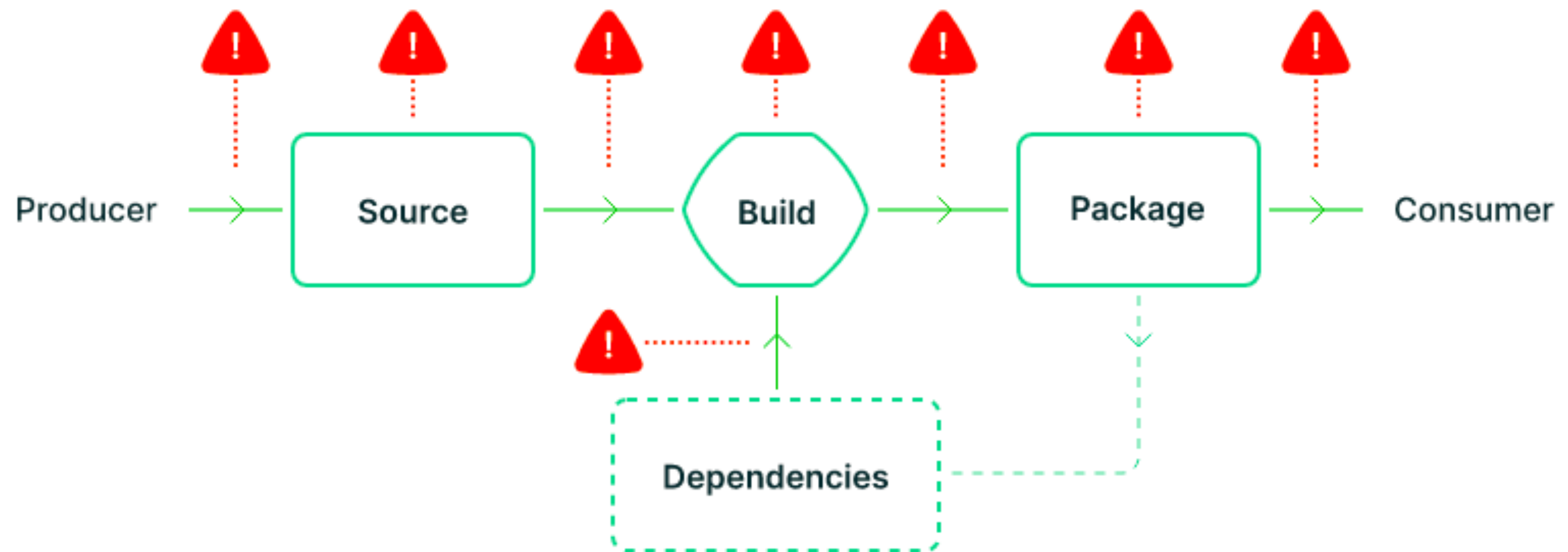
on Oct 8, 2022

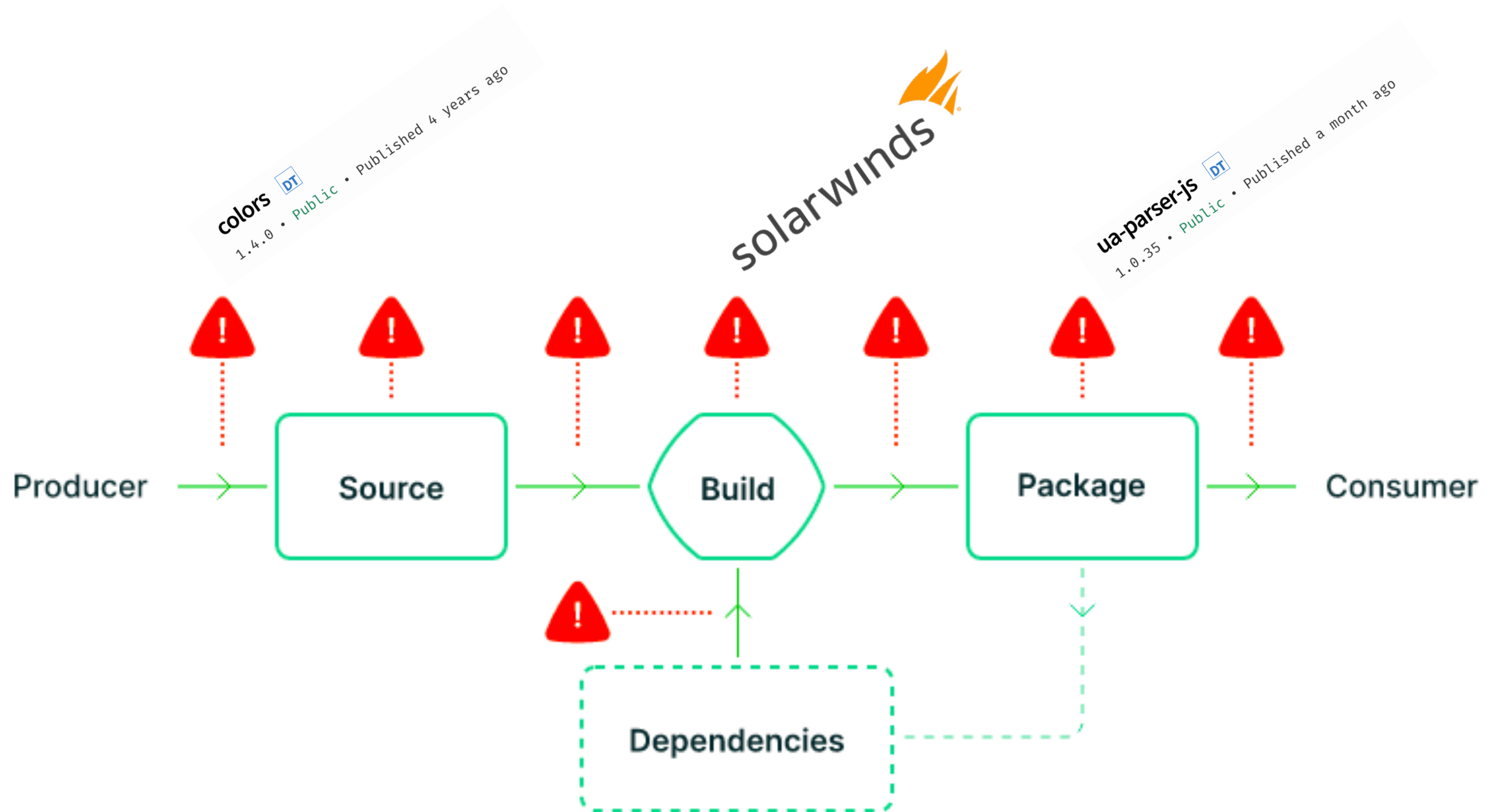
+ 146 releases

Packages

No packages published

# Supply chain







# Build levels

In order to produce artifacts with a specific build level, responsibility is split between the **Producer** and **Build platform**. The build platform **MUST** strengthen the security controls in order to achieve a specific level while the producer **MUST** choose and adopt a build platform capable of achieving a desired build level, implementing any controls as specified by the chosen platform.

Implementer	Requirement	Degree	L1	L2	L3
Producer	Choose an appropriate build platform		✓	✓	✓
	Follow a consistent build process		✓	✓	✓
	Distribute provenance		✓	✓	✓
Build platform	Provenance generation	Exists	✓	✓	✓
		Authentic		✓	✓
		Unforgeable			✓
	Isolation strength	Hosted		✓	✓
		Isolated			✓

# **npm publish --provenance**

- Verifiable signed link back to the commit in the source code
- Verifiable signed description of the build environment





Search packages

Search



retire



4.2.1 • Public • Published 6 days ago

Readme

Code

Beta

6 Dependencies

18 Dependents

116 Versions

Settings

Command line scanner looking for use of known vulnerable js files and node modules in web projects and/or node projects.

Install

```
npm install -g retire
```

Usage

Usage: retire [options]

Options:

- V, --version output the version number
- v, --verbose Show identified files (by default only vulnerable files)
- c, --nocache Don't use local cache
- jspath <path> Folder to scan for javascript files
- path <path> Folder to scan for both
- isrepo <path/url> Local or internal version of repo. Can be multiple

Install

```
> npm i retire
```

Repository

github.com/RetireJS/retire.js

Homepage

github.com/RetireJS/retire.js#readme

Weekly Downloads

50,937



Version

4.2.1



License

Apache-2.0

Unpacked Size

72.3 kB

Total Files

30

the version number  
entified files (by default only vulnerabl  
se local cache  
to scan for javascript files  
to scan for both  
r internal version of repo. Can be multip  
use for local cache instead of /tmp/.ret  
rl (http://some.host:8080)  
ormats: text, json, jsonsimple, depcheck  
which output should be written  
olimited list of paths to ignore

 [github.com/RetireJS/retire.js](https://github.com/RetireJS/retire.js)

Homepage

 [github.com/RetireJS/retire.js#readme](https://github.com/RetireJS/retire.js#readme)

↓ Weekly Downloads

50,937



Version

4.2.1 

License

Apache-2.0



Built and signed on  
**GitHub Actions**

[View more details](#)

Total Files

30

Pull Requests

3

0

Last publish

# Source code / Reporting an issue


The source code and issue tracker can be found at <https://github.com/RetireJS/retire.js>

## Keywords

[sbom](#) [sbom-tool](#) [sbom-generator](#) [security](#) [cli](#) [software-composition-analysis](#)  
[sca](#)

## Provenance Beta

Built and signed on

**GitHub Actions**

[View build summary.](#)

[Share feedback](#)

Source Commit [github.com/RetireJS/retire.js@44e51f](https://github.com/RetireJS/retire.js@44e51f)

Build File [.github/workflows/publish.yml](https://github.com/RetireJS/retire.js/blob/master/.github/workflows/publish.yml)

Public Ledger [Transparency log entry.](#)

Link to github commit

Link to build script

Link to transparency log

Link to github action log



### Support

[Help](#)

[Advisories](#)

### Company

[About](#)

[Blog](#)

### Terms & Policies

[Policies](#)

[Terms of Use](#)



# Transparency Log Entry

Build description

Repo and commit

Build log

```
data:
  Serial Number: '0x27bac54291e6177353ec40c88d355d0f8ad65a15'
Signature:
  Issuer: 0=sigstore.dev, CN=sigstore-intermediate
  Validity:
    Not Before: 6 days ago (2023-05-02T16:39:28+02:00)
    Not After: 6 days ago (2023-05-02T16:49:28+02:00)
  Algorithm:
    name: ECDSA
    namedCurve: P-256
  Subject:
    extraNames:
      items: {}
    asn: []
X509v3 extensions:
  Key Usage (critical):
    - Digital Signature
  Extended Key Usage:
    - Code Signing
  Subject Key Identifier:
    - 5D:71:05:CB:8B:CB:6D:ED:63:F4:0A:E5:30:D0:E0:9B:ED:38:4C:B7
  Authority Key Identifier:
    keyid: DF:D3:E9:CF:56:24:11:96:F9:A8:D8:E9:28:55:A2:C6:2E:18:64:3F
  Subject Alternative Name (critical):
    url:
      - https://github.com/RetireJS/retire.js/.github/workflows/publish.yml@refs/tags/4.2.1
OIDC Issuer: https://token.actions.githubusercontent.com
GitHub Workflow Trigger: release
GitHub Workflow SHA: 44e51f415af715fce27a2655899dc8fffab7f76c
GitHub Workflow Name: Publish Package to npmjs
GitHub Workflow Repository: RetireJS/retire.js
GitHub Workflow Ref: refs/tags/4.2.1
OIDC Issuer (v2): https://token.actions.githubusercontent.com
Build Signer URI: https://github.com/RetireJS/retire.js/.github/workflows/publish.yml@refs/tags/4.2.1
Build Signer Digest: 44e51f415af715fce27a2655899dc8fffab7f76c
Runner Environment: github-hosted
Source Repository URI: https://github.com/RetireJS/retire.js
Source Repository Digest: 44e51f415af715fce27a2655899dc8fffab7f76c
Source Repository Ref: refs/tags/4.2.1
Source Repository Identifier: '12496161'
Source Repository Owner URI: https://github.com/RetireJS
Source Repository Owner Identifier: '10753675'
Build Config URI: https://github.com/RetireJS/retire.js/.github/workflows/publish.yml@refs/tags/4.2.1
Build Config Digest: 44e51f415af715fce27a2655899dc8fffab7f76c
Build Trigger: release
Run Invocation URI: https://github.com/RetireJS/retire.js/actions/runs/4862487695/attempts/1
1.3.6.1.4.1.11129.2.4.2: 04:7b:00:79:00:77:00:dd:3d:30:6a:c6:c7:11:32:63:19:1e:1c:99:67:37:02:a2:4a:5e:b8:de:3c:ad:ff:87:8a:72:80:2f:29:ee:8e:00
```

# npm provenance

- This
  - links the package to the commit
  - links the package to the build
- This does not
  - protect against backdoors added by the developers or through account take-over on repo-side
  - directly protect against a compromised build-environment

# Resources

- <https://github.com/Marak/colors.js/issues/285>
- <https://krebsonsecurity.com/2021/01/solarwinds-what-hit-us-could-hit-others/>
- <https://github.com/advisories/GHSA-pjwm-rvh2-c87w>
- <https://slsa.dev/>
- <https://github.blog/2023-04-19-introducing-npm-package-provenance/>