



KubeCon



CloudNativeCon

Europe 2026

#KubeCon #CloudNativeCon

A Bug's-Eye View

Kubernetes SIG Security Explains It All





KubeCon



CloudNativeCon

Europe 2026

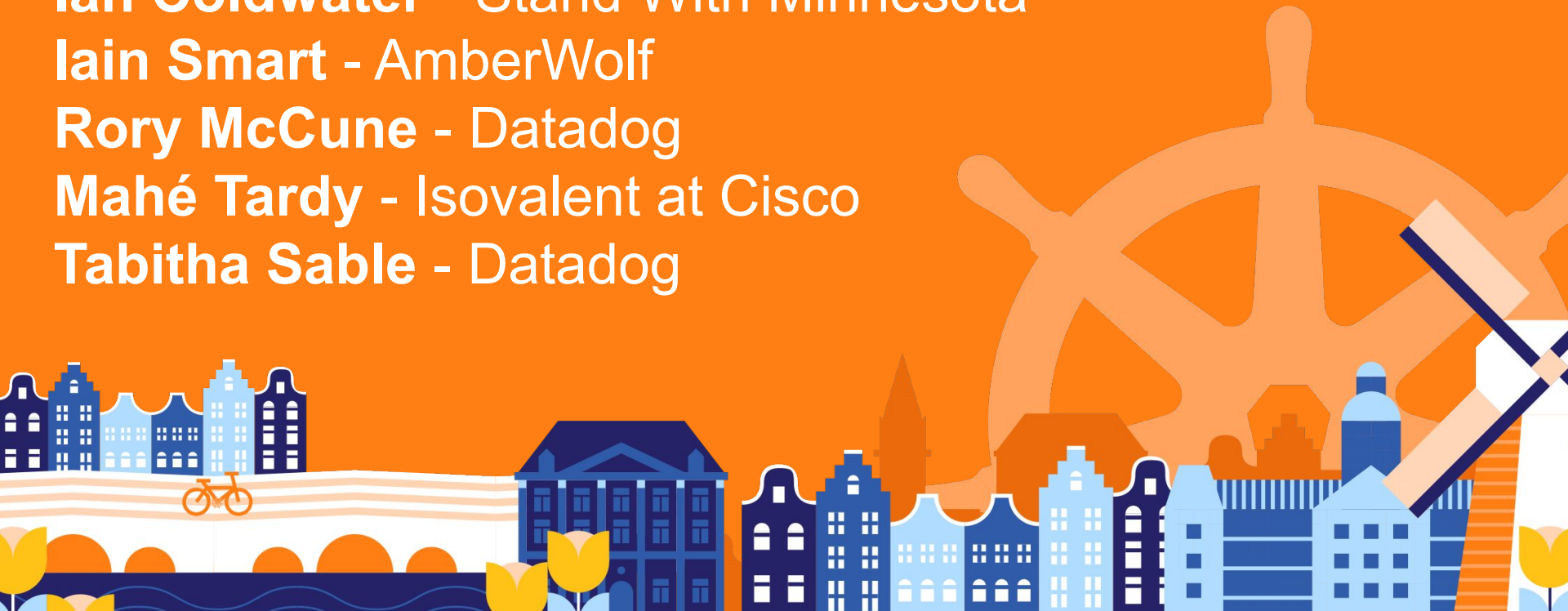
Ian Coldwater - Stand With Minnesota

Iain Smart - AmberWolf

Rory McCune - Datadog

Mahé Tardy - Isovalent at Cisco

Tabitha Sable - Datadog





KubeCon



CloudNativeCon

Europe 2026

Kubernetes SIG Security

Making Kubernetes more secure, together!



KubeCon



CloudNativeCon

Europe 2026

SIG Security Docs

What is SIG Security Docs



KubeCon



CloudNativeCon

Europe 2026

SIG Security Docs works across SIGs to improve the security content of Kubernetes documentation, as well as independently create security docs in the form of concepts/blogs



KubeCon



CloudNativeCon

Europe 2026

OWASP Kubernetes Top Ten



KubeCon



CloudNativeCon

Europe 2026

Top 10 Kubernetes Risks - 2025

2025 Top 10 Risks now available Feedback welcome. Please open issues or PRs for changes

- K01: Insecure Workload Configurations
- K02: Overly Permissive Authorization Configurations
- K03: Secrets Management Failures
- K04: Lack Of Cluster Level Policy Enforcement
- K05: Missing Network Segmentation Controls
- K06: Overly Exposed Kubernetes Components
- K07: Misconfigured And Vulnerable Cluster Components
- K08: Cluster To Cloud Lateral Movement
- K09: Broken Authentication Mechanisms
- K10: Inadequate Logging And Monitoring



KubeCon



CloudNativeCon

Europe 2026

Third-Party Audit

What is SIG Third Party Audit



KubeCon



CloudNativeCon

Europe 2026

SIG Security Audit subproject helps run
regular 3rd party audits



KubeCon



CloudNativeCon

Europe 2026

Issue Tracking and Labelling



KubeCon



CloudNativeCon

Europe 2026

We've Completed Another Audit

Huge thanks to Shielder for the hard work

Defining Scope



KubeCon



CloudNativeCon

Europe 2026



2.5 million lines of code !

Asked SIGs

Alternate audit scope
core and non-core

External Audit Roadmap
k/sig-security

65 stable features graduated
between v1.24 and v1.31



93 features / areas
initially identified



<https://github.com/kubernetes/sig-security/blob/main/sig-security-external-audit/security-audit-2025/RFP.md>

Defining Scope



KubeCon



CloudNativeCon

Europe 2026

Cluster API

Pod Security Admission

Multiple Windows Components: main
repository and csi-proxy

Konnectivity

Shared Public Cloud Library

Credential Provider Plugin

Image Builder

CEL for Admission Control /

ValidatingAdmissionPolicy & CRD Validation
Expression

Ephemeral Containers

Cgroups v2

Seccomp By Default

Node Topology Manager

Third Party Device Monitoring Plugins

AppArmor Support

Local Ephemeral Storage Capacity Isolation b8

Cleaning Up iptables Chain Ownership

kOps



KubeCon



CloudNativeCon

Europe 2026

Security Response Committee



KubeCon



CloudNativeCon

Europe 2026

...what IS a vulnerability?





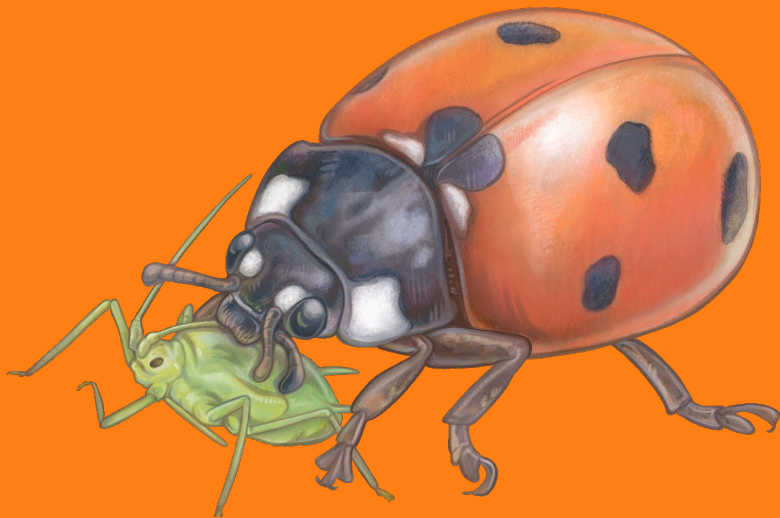
KubeCon



CloudNativeCon

Europe 2026

Sometimes it's a feature!





KubeCon



CloudNativeCon

Europe 2026

Reporting and Scoring

CVSS Scoring



KubeCon



CloudNativeCon

Europe 2026

Base Score

Attack Vector (AV)

Network (N)

Adjacent (A)

Local (L)

Physical (P)

Attack Complexity (AC)

Low (L)

High (H)

Privileges Required (PR)

None (N)

Low (L)

High (H)

User Interaction (UI)

None (N)

Required (R)

Scope (S)

Unchanged (U)

Changed (C)

Confidentiality (C)

None (N)

Low (L)

High (H)

Integrity (I)

None (N)

Low (L)

High (H)

Availability (A)

None (N)

Low (L)

High (H)

Select values
for all base
metrics to
generate
score



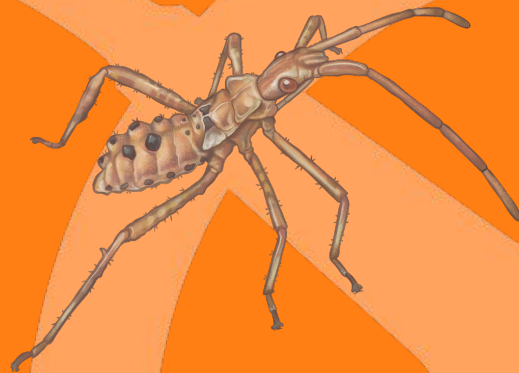
KubeCon



CloudNativeCon

Europe 2026

SIG Security Tooling



What is SIG Security Tooling?



KubeCon



CloudNativeCon

Europe 2026

SIG Security Tooling makes Kubernetes more secure with code that is community maintained with other SIGs.



KubeCon



CloudNativeCon

Europe 2026

Q Search this site

- ▶ Documentation
- ▶ Getting started
- ▶ Concepts
- ▶ Tasks
- ▶ Tutorials
- ▼ Reference
 - Glossary
 - ▶ API Overview
 - ▶ API Access Control
 - ▶ Well-Known Labels, Annotations and Taints

[Kubernetes Documentation](#) / [Reference](#) / [Kubernetes Issues and Security](#) / CVE feed

Official CVE Feed

FEATURE STATE: Kubernetes v1.27 [beta]

This is a community maintained list of official CVEs announced by the Kubernetes Security Response Committee. See [Kubernetes Security and Disclosure Information](#) for more details.

The Kubernetes project publishes a programmatically accessible feed of published security issues in [JSON feed](#) and [RSS feed](#) formats. You can access it by executing the following commands:

ISON feed

RSS feed

[Link to JSON format](#)

- [Edit this page](#)
- [Create child page](#)
- [Create an issue](#)
- [Print entire section](#)

sig-security
 sig-security-snyk-scan
 sig-security-cve-feed

[Summary](#) | **ci-kubernetes-snyk-master**

prowjob_name: ci-kubernetes-snyk-master prowjob_config_url: https://git.k8s.io/test-infra/config/jobs/kubernetes/sig-security/snyk-scan.yaml prowjob_description: Run snyk scan on k/k master periodically

03-23 04:47 CET @2035926073924915200 -- 03-08 10:14 CET @2030572635003293696; Served 120 results in 0.23 seconds

About ▾	Size ▾	Options ▾	Graph ▾	03-23				03-22				03-21				03-20			
				04:47 CET	22:46 CET	16:46 CET	10:45 CET	04:45 CET	22:44 CET	16:43 CET	10:43 CET	04:43 CET	22:43 CET	16:42 CET	10:41 CET	04:41 CET	22:40 CET	16:39 CET	10:39 CET
Local Time: ON	Display Clustered Failures List			203592607...	203583522...	203574462...	203565377...	203556317...	203547232...	203538148...	203529088...	203520028...	203510968...	203501883...	203492798...	203483673...	203474548...	203465423...	203456298...
ci-kubernetes-snyk-master.Overall																			
ci-kubernetes-snyk-master.Pod																			

New tooling working with the SRC



KubeCon



CloudNativeCon

Europe 2026

tooling: add new CLI for CVE publication by SRC members #171

Code

Merged k8s-ci-robot merged 27 commits into [kubernetes:main](#) from [mtardy:pr/mtardy/src-cve-tool](#) on Feb 6

Conversation 17

Commits 27

Checks 0

Files changed 23

+3,197



mtardy commented on Nov 1, 2025 · edited

Member

This is in reaction to [#169](#) (comment).

In short, the official CVE feed draws its information from the k/k CVE issues. People asked for us to provide a more structured information like OSV (right now the information is mostly targeted at human, even in the RSS and JSON feeds). People have been manually maintaining the OSV format for the CVE but we would like to automate it so the way we found was to provide the SRC person writing the issue with tooling that would automatically generate a JSON blob in the issue that we can parse. The first example of this was this CVE on which Tabitha used the new tool: [kubernetes/kubernetes#136680](#). You can see it generated the usual template plus a little HTML detail thing with "OSV format" at the end.

By using curl to fetch the issue content:

```
curl -L \  
-H "Accept: application/vnd.github+json" \  
-H "X-GitHub-API-Version: 2022-11-28" \  
https://api.github.com/repos/kubernetes/kubernetes/issues/136680
```

You can see that the body finishes with an HTML comment:

```
</details>\n\n<!-- generated by srcctl v1.0.0 (2665728667a5-dirty, 2026-01-31T19:18:07Z, go1.25.6) -->
```

For more details on the PR itself, it's basically this very large commit [a7d416b](#) ("new: add SRC tooling to declare new CVEs"), that took me some hours of works on many weeks of back and forth with people trying during the SIG security

Reviewers

cailyn-codes

tabbysable

Assignees

PushkarJ

tabbysable

Labels

[approved](#) [cncf-cla: yes](#) [lgtm](#) [size/XXL](#)

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

New tooling working with the SRC



KubeCon



CloudNativeCon

Europe 2026

```
=====
```

```
CVE-2026-010101
```

```
(0) Summary:
```

```
(1) CVSS: "https://www.first.org/cvss/[...]:H/PR:L/UI:N/S:U/C:L/I:L/A:L"
```

```
(2) Description:
```

```
(3) Am I vulnerable?: "Yes you are, we all are"
```

```
(4) Affected Versions:
```

```
(5) How to upgrade?:
```

```
(6) How to mitigate?:
```

```
(7) Detection:
```

```
(8) Additional Details:
```

```
(9) Acknowledgements:
```

```
(a) GitHub Issue:
```

```
(b) Fix Lead: "Mahe Tardy"
```

```
Status: successfully exported to: CVE-2026-010101.issue.md, CVE-2026-010101.email.md, CVE-2026-010101.slack.md
```

```
Enter or (0-9,a-b) to edit, (s)ave, e(x)port, (q)uit: 'x' (i)ssue, e(m)ail, (s)lack or (a)ll? █
```

New tooling working with the SRC



KubeCon



CloudNativeCon

Europe 2026

CVE-2026-4342: ingress-nginx comment-based nginx configuration injection #137893

New issue



Closed



tabbysable opened 3 days ago · edited by tabbysable

Edits

Member



CVSS Rating: 8.8 (Medium) [CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H](#)

A security issue was discovered in ingress-nginx where a combination of Ingress annotations can be used to inject configuration into nginx. This can lead to arbitrary code execution in the context of the ingress-nginx controller, and disclosure of Secrets accessible to the controller. (Note that in the default installation, the controller can access all Secrets cluster-wide.)

Am I vulnerable?

This issue affects ingress-nginx. If you do not have ingress-nginx installed on your cluster, you are not affected. You can check this by running `kubectl get pods --all-namespaces --selector app.kubernetes.io/name=ingress-nginx`.

Affected Versions

- ingress-nginx: < v1.13.9
- ingress-nginx: < v1.14.5
- ingress-nginx: < v1.15.1

How do I mitigate this vulnerability?

How to upgrade?

To upgrade, refer to the documentation: [Upgrading Ingress-nginx](#)

Assignees

No one assigned

Labels

[area/security](#) [committee/security-response](#) [kind/bug](#) [lifecycle/frozen](#) [official-cve-feed](#) [sig/network](#) [triage/accepted](#)

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

New tooling working with the SRC



KubeCon



CloudNativeCon

Europe 2026

🔒 Closed

CVE-2026-4342: ingress-nginx comment-based nginx configuration injection #137893



Acknowledgements

This vulnerability was reported by wooseokdotkim.

/triage accepted

/lifecycle frozen

/area security

/kind bug

/committee security-response

▼ OSV format

```
{
  "schema_version": "1.6.0",
  "id": "CVE-2026-4342",
  "modified": "2026-03-19T17:11:29Z",
  "summary": "ingress-nginx comment-based nginx configuration injection",
  "details": "A security issue was discovered in ingress-nginx where a combination of Ingress annotations can be",
  "severity": {
    {
      "type": "CVSS_V3",
      "score": "CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H"
    }
  ],
  "affected": [
    {
      "package": {
        "ecosystem": "Kubernetes",
        "name": "ingress-nginx"
      },
      "ranges": [
        {
          "type": "SEMVER",
          "events": [
            {
              "introduced": "0"
            }
          ],
          "fixed": "v1.13.0"
        }
      ]
    }
  ]
}
```

Labels

area/security

committee/security-response

kind/bug

lifecycle/frozen

official-cve-feed

sig/network

triage/accepted

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development



Code with agent mode

No branches or pull requests

Notifications

Customize



Subscribe

You're not receiving notifications from this thread.

Participants

Disclosure of updates to old CVEs



KubeCon



CloudNativeCon

Europe 2026

Coordinated disclosure of updates to historical CVE records #184

New issue



Open



tabbysable opened 3 weeks ago

Member ...

Kubernetes has a few CVEs that will not be fixed (see also [kubernetes/committee-security-response#220](#)), and the metadata of those CVEs is incorrect. I believe that this error results in the CVEs not showing up for k8s versions that are affected.

Before we update that metadata to be correct, we should write up a blog post and announce a date for when the correction will be made.



tabbysable 3 weeks ago

Member Author ...

/triage accepted
/assign @PushkarJ



k8s-ci-robot assigned PushkarJ 3 weeks ago

k8s-ci-robot added **triage/accepted** 3 weeks ago

tabbysable self-assigned this 3 weeks ago

tabbysable mentioned this 3 weeks ago

Update Records for Unfixed CVEs: CVE-2020-8561. CVE-2020-8562 & CVE-2021-25740 committee-security-

Assignees



PushkarJ



tabbysable

Labels

triage/accepted

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with agent mode

No branches or pull requests

Notifications

Customize

Subscribe

Shout-outs to SIG Security Tooling Contributors



KubeCon

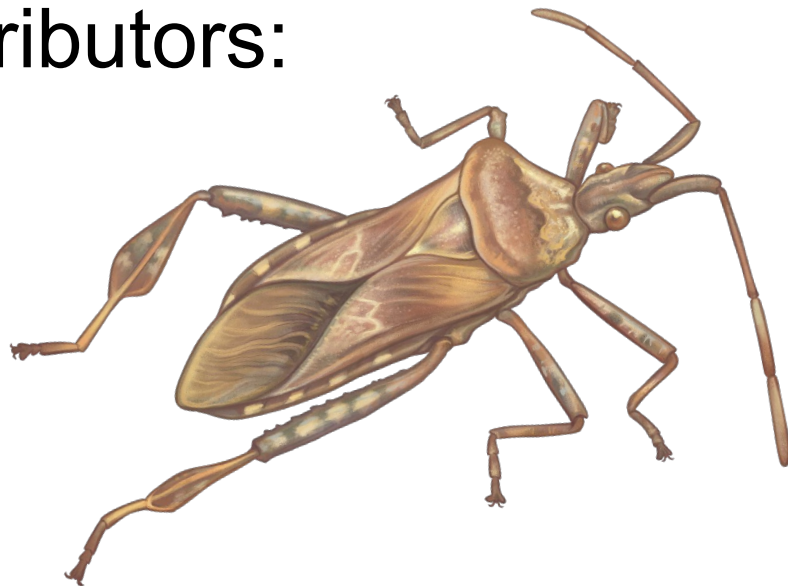


CloudNativeCon

Europe 2026

Shout-outs to our contributors:

- Arivappa
- Sherine
- Eric
- Pushkar
- Tabitha



Become a tooling contributor!



KubeCon

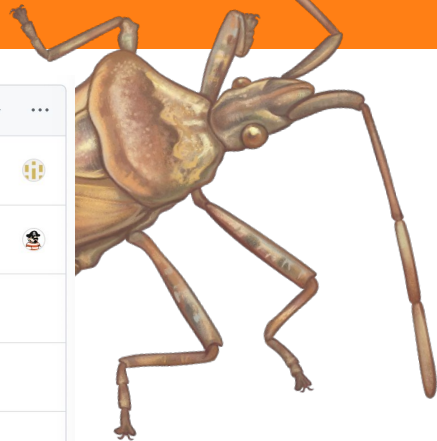


CloudNativeCon

Europe 2026

We meet
every two
weeks on
Fridays at
17:00
CET.

Open	10	Closed	25	Author	Labels	Projects	Milestones	Assignees	Types	...
Open	10	Closed	25							
tooling: add a README.md to sig-security-tooling/srctl	1	8		#176 · mtardy opened on Feb 6						
tooling: run tests and linters with prow for srctl	1	8		#175 · mtardy opened on Feb 6	good first issue	help wanted				
tooling: add the OSV CVE information to the official CVE feed	1			#177 · mtardy opened on Feb 6						
tooling: include new CVE issues JSON OSV blob information in the CVE feed	1	4		#179 · mtardy opened on Feb 6	sig/security					
tooling: include kubernetes-sigs/cve-feed-osv OSV information in the CVE feed	1	4		#178 · mtardy opened on Feb 6	sig/security					
Umbrella issue: Migrate CVE feed to run under cloud build		2		#150 · tabbysable opened on Aug 1, 2025	triage/accepted					
Scanning and private triage of dangling DNS records	1	5		#172 · tabbysable opened on Nov 8, 2025	help wanted	sig/security	triage/accepted			
TODO: create dedicated google group for CVE feed maintainers	1	3		#149 · tabbysable opened on Aug 1, 2025	triage/accepted					
Create a periodically auto-refreshing list of fixed CVEs		57		#1 · PushkarJ opened on Jul 30, 2021	sig/security	committee/security-response	sig/docs	sig/release		
[govulncheck] Generate VEX documents from govulncheck output		30		#116 · PushkarJ opened on Jun 28, 2024	sig/architecture	sig/docs	sig/release	sig/security	area/dependency	kind/feature





KubeCon



CloudNativeCon

Europe 2026

Get Involved!





KubeCon



CloudNativeCon

Europe 2026

