

































-  Secrets
-  ABAP
-  Apex
-  C
-  C++
-  CloudFormation
-  COBOL
-  C#
-  CSS
-  Flex
-  Go
-  HTML
-  Java
-  JavaScript
-  Kotlin
-  **Kubernetes**
-  Objective C
-  PHP
-  PL/I
-  PL/SQL
-  Python
-  RPG
-  Ruby
-  Scala
-  Swift
-  Terraform
-  Text
-  TypeScript
-  T-SQL
-  VB.NET
-  VB6
-  XML



Kubernetes static code analysis

Unique rules to find Security Hotspots in your KUBERNETES code

- All rules7
-  Security Hotspot6
-  Code Smell1

Tags

Search by name...



Mounting sensitive file system paths is security-sensitive

 Security Hotspot

Using host operating system namespaces is security-sensitive

 Security Hotspot

Allowing process privilege escalations is security-sensitive

 Security Hotspot

Exposing Docker sockets is security-sensitive

 Security Hotspot


Running containers in privileged mode is security-sensitive

 Security Hotspot

Setting capabilities is security-sensitive

 Security Hotspot

Kubernetes parsing failure

 Code Smell

Running containers in privileged mode is security-sensitive

Analyze your code

 Security Hotspot  Major  cwe

Running containers in privileged mode can reduce the resilience of a cluster in the event of a security incident because it weakens the isolation between hosts and containers.

Process permissions in privileged containers are essentially the same as root permissions on the host. If these processes are not protected by robust security measures, an attacker who compromises a root process on a Pod's host is likely to gain the ability to pivot within the cluster. Depending on how resilient the cluster is, attackers can extend their attack to the cluster by compromising the nodes from which the cluster launched the process.

Ask Yourself Whether

- The services of this Pod are accessible to people who are not administrators of the Kubernetes cluster.

There is a risk if you answered yes to any of those questions.

Recommended Secure Coding Practices

Disable privileged mode.

Sensitive Code Example

```
apiVersion: v1
kind: Pod
metadata:
  name: example
spec:
  containers:
    - name: web
      image: nginx
      ports:
        - name: web
          containerPort: 80
          protocol: TCP
      securityContext:
        privileged: true # Sensitive
```

Compliant Solution

```
apiVersion: v1
kind: Pod
metadata:
  name: example
spec:
  containers:
    - name: web
      image: nginx
      ports:
        - name: web
          containerPort: 80
          protocol: TCP
      securityContext:
```

privileged: false

See

- [MITRE, CWE-284](#) - Improper Access Control

Available In:

