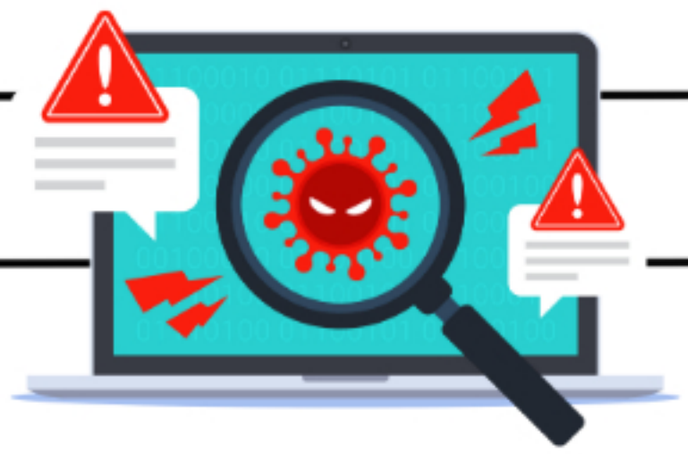
OWASP

K8s Top 10 Risks

OWASP

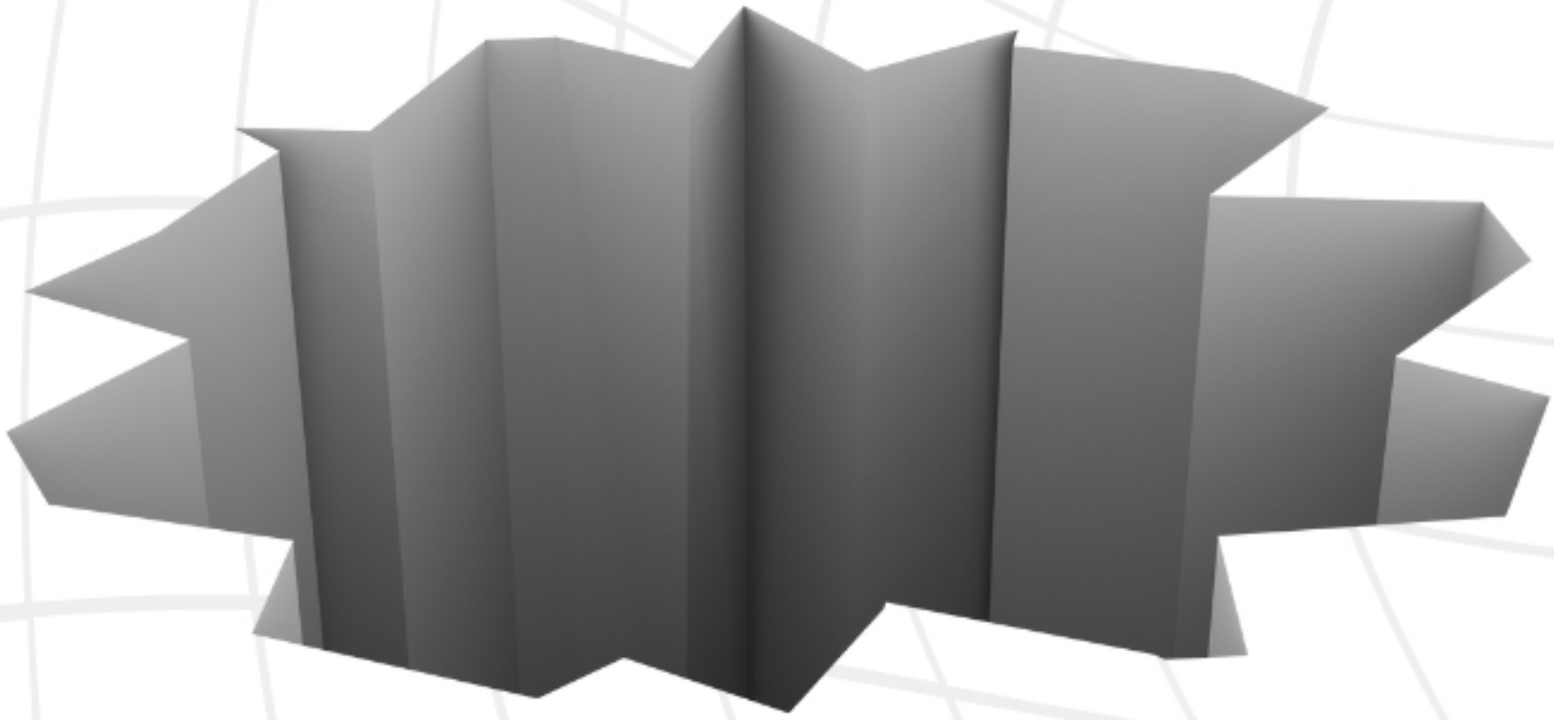
Open Web Application Security Project

The OWASP Kubernetes Top 10 is a prioritized list of the most common security risks associated with Kubernetes.



kubernetes

Here are 10 cloud-native K8s threats you'll want to avoid:



1 Insecure Workload Configurations

In Kubernetes, complex workload configurations can lead to security risks if misconfigured, like granting excessive privileges.

---

2 Supply Chain Vulnerabilities

Supply chain threats in Kubernetes are significant due to dependencies in container runtime and build cycle, making them susceptible to malicious code.

3 Overly Permissive RBAC Configurations

Incorrect RBAC configuration in Kubernetes can lead to broad compromises by not adhering to the least privilege model.

---

4 Lack of Centralized Policy Enforcement

Without centralized policy management, Kubernetes governance and compliance can be compromised, allowing for potential security breaches.

5 Inadequate Logging and Monitoring

In Kubernetes, inadequate logging and monitoring can leave attackers undetected, making active monitoring and auditing essential.

6 Broken Authentication Mechanisms

In Kubernetes, vulnerabilities in authentication mechanisms can expose the system to unauthorized access.

7 Missing Network Segmentation Controls

A lack of network segmentation in Kubernetes can allow attackers to move laterally within a compromised cluster.

8 Secrets Management Failures

In Kubernetes, improperly managed secrets, like unencrypted sensitive data, can lead to security breaches.

9 Misconfigured Cluster Components

Insecure configurations of Kubernetes' core components can lead to escalated privileges and security risks.

10 Outdated and Vulnerable Kubernetes Components

Regularly updating Kubernetes components is crucial to protect against vulnerabilities, as the ecosystem is prone to frequent CVEs.