Information leak via AdmissionPolicyGroup Resource

Moderate **flavio** published **GHSA-756x-m4mj-q96c** 2 weeks ago

Package	Affected versions	Patched versions
kubewarden-controller (kubewarden)	>= 1.17.0	1.21.0

Description

Impact

The policy group feature, added to by the 1.17.0 release, introduced two new types of CRD: ClusterAdmissionPolicyGroup and AdmissionPolicyGroup. The former is cluster wide, while the latter is namespaced.

By being namespaced, the AdmissionPolicyGroup has a well constrained impact on cluster resources. Hence, it's considered safe to allow non-admin users to create and manage these resources in the namespaces they own. Kubewarden policies can be allowed to query the Kubernetes API at evaluation time; these types of policies are called "context aware". Context aware policies can perform list and get operations against a Kubernetes cluster. The queries are done using the ServiceAccount of the Policy Server instance that hosts the policy. That means that access to the cluster is determined by the RBAC rules that apply to that ServiceAccount. The AdmissionPolicyGroup CRD allowed the deployment of context aware policies. This could allow an attacker to obtain information about resources that are out of their reach, by leveraging a higher access to the cluster granted to the ServiceAccount token used to run the policy.

The impact of this vulnerability depends on the privileges that have been granted to the ServiceAccount used to run the Policy Server and assumes that users are using the recommended best practices of keeping the Policy Server's ServiceAccount least privileged. By default, the Kubewarden helm chart grants access to the following resources (cluster wide) only: Namespace, Pod, Deployment and Ingress.

Patches

Severity

Moderate 4.3 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	None
Availability	None

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

CVE ID

CVE-2025-24784

Weaknesses

No CWEs

Credits

 **flavio** Finder

Starting from the 1.21.0 release, the AdmissionPolicyGroup CRD does not allow the definition of context aware policies. No modifications are needed neither for performing the upgrade nor afterwards.

Workarounds

On clusters running Kubewarden < 1.21.0, the following Kubewarden policy can be applied to prevent the creation of AdmissionPolicyGroup resources that have access to Kubernetes resources:

```yaml
apiVersion: policies.kubewarden.io/v1
kind: ClusterAdmissionPolicy
metadata:
  name: "deny-admission-policy-groups-with-context-resources"
spec:
  module: registry://ghcr.io/kubewarden/policies/cel-policy:latest
  settings:
    variables:
      - name: hasContextAwareResources
        expression: "object.spec.policies.exists(p, has(object.spec.p
      - name: isPendingDeletion
        expression: "has(object.metadata.deletionTimestamp)"
    validations:
      - expression: "!variables.hasContextAwareResources || variables
        message: "AdmissionPolicyGroup has contextAwareResources defi
  rules:
    - apiGroups: ["policies.kubewarden.io"]
      apiVersions: ["v1"]
      operations: ["CREATE", "UPDATE"]
      resources: ["admissionpolicygroups"]
  mutating: false
  backgroundAudit: true
```

Once the policy is applied, the Kubewarden Audit Scanner can be used to identify the AdmissionPolicyGroup policies that are violating this policy.

For more information

If you have any questions or comments about this advisory you can contact the Kubewarden team using the procedures described under the “security disclosure“ guidelines of the Kubewarden project.