BMO can expose any secret from other namespaces via BMCEventSubscription CRD

Moderate **tuminoid** published **GHSA-c98h-7hp9-v9hq** 5 days ago

Package	Affected versions	Patched versions
github.com/metal3-io/baremetal-operator/apis (Go)	v0.9.0, <=v0.8.0	v0.9.1, v0.8.1

Description

Impact

The Bare Metal Operator (BMO) implements a Kubernetes API for managing bare metal hosts in Metal3.

Baremetal Operator enables users to load Secret from arbitrary namespaces upon deployment of the namespace scoped Custom Resource `BMCEventSubscription` (BMCES). An adversary Kubernetes account with only namespace level roles (e.g. a tenant controlling a namespace) may create a BMCES in their authorized namespace and then load Secrets from their unauthorized namespaces to their authorized namespace via the Baremetal Operator controller's cluster scoped privileges, causing Secret leakage.

Patches

The patch makes BMO refuse to read Secrets from other namespace than where the corresponding Bare Metal Host (BMH) resource is. The patch does not change the `BMCEventSubscription` API in BMO, but stricter validation will deny the request at admission time. It will also prevent the controller reading such Secrets, in case the BMCES resource has already been deployed.

The issue exists for all versions of BMO, and is patched in BMO releases v0.9.1 and v0.8.1. Prior upgrading to patched BMO version, duplicate any existing Secret pointed to by `BMCEventSubscription`'s `httpHeadersRef` to the same namespace where the corresponding BMH exists. After upgrade, remove the old Secrets.

Severity

Moderate 6.5 / 10

CVSS v3 base metrics

Attack vector	Local
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	None
Availability	None

Learn more about base metrics

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

CVE ID

CVE-2025-29781

Weaknesses

CWE-200 CWE-653

Credits

debuggerchen Reporter

Workarounds

Operator can configure BMO RBAC to be namespace scoped, instead of cluster scoped, to prevent BMO from accessing Secrets from other namespaces, and/or use `WATCH_NAMESPACE` configuration option to limit BMO to single namespace.

References

- patch to main
- patch to release-0.9
- patch to release-0.8
- BMCEventSubscription design document

Credits

Metal3 Security Team thanks WHALEEYE and debuggerchen of Lab for Internet and Security Technology for responsible vulnerability disclosure.