

[GitHub Advisory Database](#) / [GitHub Reviewed](#) / CVE-2024-5042

Submariner Operator sets unnecessary RBAC permissions

Moderate severity

GitHub Reviewed

Published on May 17, 2024 to the GitHub Advisory Database •

Updated 3 weeks ago

Vulnerability detailsDependabot alerts **0**

Package

github.com/submariner-io/submariner-operator (Go)

Affected versions

>= 0.16.0-m0, < 0.16.4

>= 0.17.0-m0, < 0.17.2

< 0.15.4

>= 0.18.0-m0, < 0.18.0-rc0

Patched versions

0.16.4

0.17.2

0.15.4

0.18.0-rc0

Description

A flaw was found in the Submariner project. Due to unnecessary role-based access control permissions, a privileged attacker can run a malicious container on a node that may allow them to steal service account tokens and further compromise other nodes and potentially the entire cluster.

References

- <https://nvd.nist.gov/vuln/detail/CVE-2024-5042>
- <https://access.redhat.com/security/cve/CVE-2024-5042>
- https://bugzilla.redhat.com/show_bug.cgi?id=2280921
- [submariner-io/submariner-operator#3041](#)
- [submariner-io/submariner-operator#3040](#)
- [submariner-io/submariner-operator@ b27a04c](#)
- <https://access.redhat.com/errata/RHSA-2024:4591>
- [submariner-io/submariner-operator#3045](#)
- [submariner-io/submariner-operator#3046](#)
- [submariner-io/submariner-operator#3049](#)
- <https://access.redhat.com/errata/RHSA-2026:6503>
- [GHSA-2rhx-qhxp-5jpw](#)



Published by the [National Vulnerability Database](#) on May 17, 2024



Published to the GitHub Advisory Database on May 17, 2024



Reviewed on May 17, 2024



Last updated 3 weeks ago

Severity

Moderate 6.6 / 10

CVSS v3 base metrics

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

[Learn more about base metrics](#)

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

EPSS score

0.064% (20th percentile)

Weaknesses

► CWE-250

CVE ID

CVE-2024-5042

GHSA ID

GHSA-2rhx-qhxp-5jpw

Source code

[submariner-io/submariner-operator](#)

Credits



skitt

Analyst

This advisory has been edited. [See History](#).

See something to contribute? [Suggest improvements for this vulnerability](#).