Bug 2280921 (CVE-2024-5042) - CVE-2024-5042 submariner-operator: RBAC permissions can allow for the spread of node compromises

Keywords: Security

Status: NEW

Alias: CVE-2024-5042

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 2290351

Blocks: 2280922

TreeView+ depends on / blocked

Reported: 2024-05-17 03:54 UTC by Robb Gatica

Modified: 2024-07-17 13:23 UTC (History)

CC List: 7 users (show)

Fixed In Version: submariner-operator 0.16.4

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments	(Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2024:4591	0	None	None	None	2024-07-17 13:23:08 UTC

Robb Gatica 2024-05-17 03:54:51 UTC Description

```
The Submariner project received a security disclosure
regarding unnecessary RBAC that could be used to spread K8s
node compromises. If an attacker is able to run a privileged
malicious container on a node, they may be able to escape the
```

container and steal service account tokens. Since Submariner's route agent runs on every node, its SA token is available from any compromised node.

References:
https://github.com/submariner-io/submariner-operator/issues/3041

errata-xmlrpc 2024-07-17 13:23:07 UTC Comment 7

This issue has been addressed in the following products:

RHODF-4.16-RHEL-9

Via RHSA-2024:4591 https://access.redhat.com/errata/RHSA-2024:4591

Note

You need to log in before you can comment on or make changes to this bug.