Weave CNI password is not configured when a cluster is created from an RKE template

Moderate **maxsokolovsky** published **GHSA-vrph-m5jj-c46c** on May 24

Package

Rancher (Rancher)

Affected versions	Patched versions
Up to and including 2.5.13 and 2.6.4	2.5.14, 2.6.5 and later releases

Description

Impact

This vulnerability only affects customers using Weave CNI (Container Network Interface) when configured through RKE templates.

A flaw was discovered in Rancher versions from 2.5.0 up to and including 2.5.13 and from 2.6.0 up to and including 2.6.4, where a UI (user interface) issue with RKE templates does not include a value for the Weave password when Weave is chosen as the CNI.

If a cluster is created based on the mentioned template and Weave is configured as the CNI, no password will be created for network encryption in Weave, therefore network traffic in the cluster will be sent unencrypted.

This issue does not happen when a cluster, with Weave configured as CNI, is created without using an RKE template.

The impact of this vulnerability is higher when nodes on the cluster are on different locations and communicate with one another through the Internet, where monitoring (sniffing) of the network traffic by third-party entities can be more easily achieved.

Patches

Patched versions include releases 2.5.14, 2.6.5 and later versions of Rancher. Besides upgrading to a Rancher patched version, the workarounds listed below must be applied in order for Weave to properly encrypt the network traffic.

Workarounds

1. A manual password can be set in Weave by directly editing Weave's DaemonSet on the affected cluster to add the `WEAVE_PASSWORD` environment variable together with the a value for the password.

```
$ kubectl -n kube-system edit ds weave-net
```

```
<snipped>
      containers:
      - command:
        - /home/weave/launch.sh
        env:
        - name: INIT_CONTAINER
          value: "true"
        - name: HOSTNAME
          valueFrom:
            fieldRef:
              apiVersion: v1
              fieldPath: spec.nodeName
        - name: IPALLOC_RANGE
          value: <IP allocation range>
        - name: WEAVE_PASSWORD
          value: "insert strong secret password here"
        image: <Weave image>
<snipped>
```

2. A new RKE template revision must be created in order to properly generate the Weave password on new clusters.

Notes

1. In order to provide protection against brute-force attacks, that might break the network encryption, a strong password must be generated for the workaround. Weave's documentation provides recommendations for generating a strong password.

2. Manually generating the password for the workaround is only needed on affected versions of Rancher. This step is not needed when creating new RKE templates on patched versions of Rancher.

For more information

If you have any questions or comments about this advisory:

- Reach out to SUSE Rancher Security team for security related inquiries.

- Open an issue in Rancher repository.
- Verify SUSE Rancher support matrix and product support lifecycle.

Severity

Moderate 6.8 / 10

CVSS base metrics

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

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

CVE ID

CVE-2022-21951

Weaknesses

CWE-311