rancher / **rancher** Public

Code Issues 2.2k Pull requests 114 Actions Projects Wiki ...

Downstream cluster privilege escalation through cluster and project role template binding (CRTB/PRTB)

Critical **rmweir** published **GHSA-6x34-89p7-95wg** on Aug 18

Package

rancher/rancher (Go)

Affected versions	Patched versions
From 2.5.0 and 2.6.0 up to and including 2.5.15 and 2.6.6	2.5.16, 2.6.7 and later releases

Description

Impact

An issue was discovered in Rancher versions up to and including 2.5.15 and 2.6.6 where a flaw with authorization logic allows privilege escalation through cluster role template binding (CRTB) and project role template binding (PRTB). This issue does not affect the local cluster, it affects only downstream clusters.

The vulnerability can be exploited by any user who has permissions to create/edit cluster role template bindings or project role template bindings (such as `cluster-owner`, `manage cluster members`, `project-owner` and `manage project members`) to gain `owner` permission in another project in the same cluster or in another project on a different downstream cluster.

- The user must have `kubectl` access in the local cluster to exploit this scenario.
- This can only be abused to gain `cluster-owner` permission on a different downstream cluster if the user is already `cluster-owner` on at least one downstream cluster.
- Example of a modified CRTB (note: the `clusterName` points to the cluster ID of the cluster that the privileges will be escalated and `namespace` points to the current cluster ID that the user has permissions):

```
kubectl edit clusterroletemplatebindings crtb-<crtb-ID> -n c-<cluster-ID>
---
apiVersion: management.cattle.io/v3
clusterName: <ID-of-the-cluster-to-escalate>
kind: ClusterRoleTemplateBinding
metadata:
  annotations:
    <omitted>
  finalizers:
  - <omitted>
  generateName: crtb-
  labels:
    <omitted>
    cattle.io/creator: norman
  name: crtb-<crtb-ID>
  namespace: c-<current-cluster-ID>
roleTemplateName: cluster-owner
userName: u-<user-ID>
userPrincipalName: local://u-<user-ID>
```

An artifact to flag the exploitation of this issue is that the `namespace` of the CRTB/PRTB will not match the cluster name (`clusterName`) of the CRTB/PRTB. For example, every CRTB in the `c-123xyz` namespace should have a cluster name of `c-123xyz` . If instead, the cluster name is `c-abc567` , for example, this is likely a result of a user exploiting this flaw.

For more information about cluster and project roles, please consult Rancher's documentation.

Patches

Patched versions include releases 2.5.16, 2.6.7 and later versions.

Workarounds

Limit access in Rancher to trusted users. There is not a direct mitigation besides upgrading to the patched Rancher versions.

Important:

- It is highly advised to check the local and downstream clusters for potential unrecognized CRTBs (`kubectl get clusterroletemplatebindings -A`) and PRTBs (`kubectl get projectroletemplatebindings -A`) assignments.
- The ability to add other users to projects and clusters is a highly-privileged permission which may result in users being able to operate beyond their explicitly specified RBAC. It is recommended that this permission be granted selectively.

The following script can be used as a helper to detect possible deviations of CRTBs and PRTBs that do not match the expected value. Further investigation is required to determine if the flagged objects were maliciously modified or not. The script requires `kubectl` access to the `local` cluster and the `jq` command.

```
#!/usr/bin/env bash

echo "CRTBs that don't match cluster:"
kubectl get clusterroletemplatebindings -A -o=jsonpath="{range .items[?(@.clusterName!=@.metadat

echo "PRTBs that don't match project:"
kubectl get projectroletemplatebindings -A -ojson | jq -r '.items[]|.metadata as $m|select(.proj
```

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 our support matrix and product support lifecycle.

Severity

Critical 9.1 / 10

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

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

CVE ID

CVE-2022-31247

Weaknesses

CWE-285