benc-uk / **kubeview** Public

Code   Issues 12   Pull requests 9   Actions   Projects   Security   ···

New issue

Jump to bottom

[CVE-2022-45933] Critical Security Issue that could lead to full cluster takeover #95

Open **OmniSl4sh** opened this issue 13 days ago · 2 comments

OmniSl4sh commented 13 days ago

Hello,

may you please consider **adding authentication** to **KubeView?**

a `curl` to the the API for the `kube-system` namespace would return certificate files that can be used for authentication and **ultimately lead to taking full control over the k8s cluster!**

the request would be like this:

```
curl http://x.x.x.x/api/scrape/kube-system | jq | grep -P '(BEGIN|END) (RSA|CERT)'
```

and using the certs for auth like below:

```
kubectl --client-certificate=adm.crt --client-key=adm.key --certificate-authority ca.crt --server https://x.x.x.x
```

Please fix this ASAP to make sure everyone who uses this is secure.

Thanks in advance :)

benc-uk commented 12 days ago Owner

Thanks for flagging this.
Kubeview created as a fun side project and a learning exercise, I knew it wasn't very secure from the start, I can see if I can find a way to exclude these from the scrape API

Sorry it won't be done ASAP as I have other priorities

OmniSl4sh commented 12 days ago Author

You're welcome.

Sure I understand.

Excuse me if I offended you by asking for this to be done ASAP. it wasn't intended.
I also didn't mean to suggest only one way for the fix: authentication. I totally respect how you want security to be implemented since it's your project.

It was out of panic and concern that's all. I'm sure you can imagine the impact if this is exposed to a malicious actor.

However, authentication would reduce the amount of information disclosure to zero which I believe is the best option. of course, I'll be glad to hear a better opinion.

I'm positive that you also won't disagree that jeopardizing the security of an entire cluster would greatly outweigh a great solution like yours. Even if it's totally open-source and free.

Kindly mind that responsibility.

Thank you again.

👍 1

OmniSl4sh changed the title ~~Critical Security Issue that could lead to full cluster takeover~~ [CVE-2022-45933] Critical Security Issue that could lead to full cluster takeover 6 days ago

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants