New issue

Kong-ingress-controller 3.4 has high CPU usage when running 2 pods #6907

Open

Labels bug

camaeel opened on Dec 29, 2024 · edited by camaeel Edits

Is there an existing issue for this?

I have searched the existing issues

Current Behavior

Recently I upgraded "ingress" helm chart (from) from version v0.16.0 to v0.17.0. This included upgrade of kong-ingress-controller from 3.3 to 3.4.
After this was upgraded **one** of 2 replicas of kong-ingress-controller started to consume 2 CPU full cores.
When I scaled to 1 replica, the only replica had low CPU usage.

Nothing interesting/repeated in the logs.

Since this is home-lab setup it has almost no traffic, so this was not caused by user traffic.

Expected Behavior

Both pods should have low CPU usage

Steps To Reproduce

On kind cluster I had bad performance even with one pod.

1. Install ingress chart from https://charts.konghq.com version v0.17.0 with 2 repl

```
    helm upgrade --install -n kong kong kong/ingress --version v0.17.0 --create-namespace
    ```
2. Observe `kubectl top`

Kong Ingress Controller version

```
4.4
```

Kubernetes version

```
Server Version: v1.30.6
```

Anything else?

No response


  **camaeel** added **bug** on Dec 29, 2024

 **mainey-cc** on Dec 29, 2024

+1, i have the exact same issue here. Some of my kong ingress controller replica are hogging 2 vCPU each (2 out of 5).

Running kong helm chart 2.46.0

 **arturo-soucase** on Jan 2

We have found this message in the logs:

```
info setup Starting controller manager. Kong does not care about security. {"v": 0,
"release": "3.4.0", "repo": "https://github.com/kong/kubernetes-ingress-
controller.git", "commit": "92a6761ac1c94ecd202571cbf84de860336664f3"}
```

😕 5

ego93 on Jan 2 · edited by ego93 Edits •••

I believe that the Kong kubernetes-ingress-controller 3.4 and 3.4.0 images have been compromised in Kongs Docker hub account and that the image has been replaced with a similar image with a crypto miner injected which would explain the high CPU.

This image was introduced in the helm chart 2.46.0 and also the ingress-0.17.0 chart.

Version 3.4 of the kong/kubernetes-ingress-controller image was released on the 18th December 2024 but the docker hub image was last updated on the 24th December 2024

👀 3

lahabana on Jan 3 · edited by lahabana Edits Contributor •••

KIC image 3.4.0 contained unauthorized code. We have released 3.4.1 which removes the unauthorized code. We also removed the tags 3.4.0 and updated latest and 3.4 to point to 3.4.1.

For added security you can use the digest for the release: http://docker.io/kong/kubernetes-ingress-controller:3.4.1@sha256:45da0da02c395bfdb6a324370b87eca39098bad42b184b57d56a44d5d95da99e
For amd: sha256:b358296fa6a1458c977c0513ff918e80b708fa9d7721f9d438f3dfce24f60f4f

For arm: sha256:e0125aa85a4c9eef7822ba5234e90958c71e1d29474d6247adc3e7e21327e8ee

Our investigation is continuing. At this point we believe the unauthorized actor exploited a misconfiguration in the KIC public repository build pipeline. We have rotated all keys and taken other measures to help ensure image integrity.

 **camaeel** on Jan 5 Author •••

@lahabana If helm charts use moving tag that point to minor version it would make sense to set by default ImagePullPolicy to Always, so in case moving tag (in this case 3.4) is updated kubernetes pulls latest image automatically.
Another option would be to pin helm chart to proper patch-level versions and then potentially also pin SHA of the images (you can pin manifest for 3.4.1 that binds both architecture images to make it universal across architectures.

 👍 3

 **ego93** on Jan 6 •••

I agree with @camaeel suggestion here, pinning to a sha and setting the ImagePullPolicy would be a wise and more secure method.

 **ego93** mentioned this on Jan 6

Pin image version to SHA of the tag Kong/charts#1208

 **AdnaneKhan** on Jan 6 · edited by AdnaneKhan Edits •••

~~Is Kong planning on releasing a formal advisory on this incident?~~ This is a very serious compromise given how many downloads the KIC image has and its role as a control plane container. It's concerning enough that this was not picked up by Kong monitoring their own release channel. ~~Not announcing this publicly borders on neglect as there are likely victims of this attack still running the malicious container in their infrastructure.~~

Time is of the essence in these scenarios.

~~At this point the community does not have:~~

~~* IOCs - SHA hashes of the compromised images. How can people know if they are running the infected version of the image?~~
~~* Remediation steps - How can someone who is running the malicious image quickly evict it from their infrastructure?~~

- Impact analysis - Has Kong had the chance to analyze what the malware did? The comments here suggest it was a crypto miner, but if the attacker pushed their own malicious Docker image then they could have added *anything*. Is there malicious outbound traffic? Any domains to check?

EDIT: Kong advisory went out a few minutes before I hit the comment button. Thank you for the transparency!

❤️ 2

mrwanny on Jan 6

A github security advisory was just issued advising the community to upgrade to 3.4.1.

👍 10

mrwanny on Jan 7

We completely understand the desire for transparency. Please know we are taking this incident extremely seriously. In addition to the advisory noted above, we've reached out to known affected customers and engaged an outside security research firm to analyze the affected image.

At this time we have identified a cryptominer as noted in the advisory, attempting to connect to pool.supportxmr.com, but have not identified any other malicious payload. Should that change we will update this thread and the advisory.

Just as importantly, we're working through a full root cause analysis to determine how the attack occurred, and to help ensure that it cannot recur. We've made good progress on this front, and once our investigation has concluded we intend to publish our findings.

ego93 on Jan 7 · edited by ego93 Edits

@mrwanny from the same container, there was also a DNS call to `pool-fr.supportxmr.com` a key message to look out for in the logs will be `Kong does not care about security` which can be found at the startup phase of the ingress-controller pod as ref here #6907 (comment)

mrwanny on Jan 10 · edited by mrwanny Edits •••

With the assistance of a third party we have completed our review of the unauthorized KIC 3.4.0 image, and have confirmed that the XMRig Miner was the sole unauthorized malicious code, and that there is no evidence of any other malicious code.
We are also making these YARA rules available for users to run against any live system.

mrwanny on Jan 14 •••

We just posted a blog post with additional details.

r0binak on Jan 23 •••

@camaeel **@mainey-cc** **@arturo-soucase** **@ego93** **@lahabana** **@mrwanny**

Hi!

I would like to ask - where can I find the vulnerable version of the image? Maybe you have it somewhere? I looked on DockerHub, but this tag is already removed there.

Add a comment

Write Preview

Use Markdown to format your comment

Paste, drop, or click to add files

Close issue Comment

Remember, contributions to this repository should follow its contributing guidelines, security policy and code of conduct.

Metadata

Assignees

No one assigned

Labels

bug

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with Copilot Agent Mode

No branches or pull requests

Notifications Customize

Subscribe

You're not receiving notifications from this thread.

Participants

 +3