



KubeCon



CloudNativeCon

Europe 2020

*Virtual*

# The Kubernetes Bug Bounty Program: What Researchers and Users Need to Know

# Who are we?



*Virtual*



Reed Loden  
Open Source Security  
**HackerOne**



Taahir Ahmed  
GKE Security  
**Google**

# What will you learn?

- What is hacking? Who are hackers?
- What is a bug bounty program?
- How does Kubernetes security work?
- What happens when a security vulnerability is reported in Kubernetes?
- How can you contribute?





KubeCon



CloudNativeCon

Europe 2020

*Virtual*

# Let's define “hacker”

# What does the internet think about hackers?



Google

hackers are|



- hackers are **real**
- hackers are **losers**
- hackers are **scum**
- hackers are **arena**
- hackers are
- hackers are **getting smarter**
- hackers are **everywhere**
- hackers are **evil**
- hackers are **us**
- hackers are **here where are you**

[Report inappropriate predictions](#)

# What do people think hackers look like?



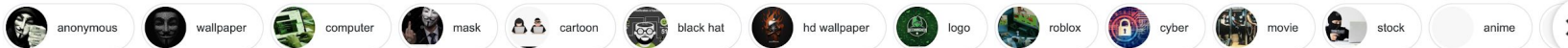
Google

hackers



All Images Videos News Maps More Settings Tools

Collections SafeSearch



The Time Hacker Method - By Carlos ...  
hackernoon.com



To Identify a Hacker, Treat Them ...  
wired.com



Most famous hackers in history - P...  
pandasecurity.com



making big bucks working for the good guys  
nypost.com



Former Hacker Mark Abene Explains the ...  
fortune.com



Iranian Hackers Increasing Their ...  
cpomagazine.com



Breach of Rust: How Hackers Break in ...  
industryweek.com



Massachusetts school district pays \$10 ...  
abcnews.go.com



Has my Gmail been hacked? How to chec...  
thesun.co.uk



Hackers are making their attacks look ...  
fifthdomain.com



North Korean hackers' evolution on ...  
asia.nikkei.com



Ryuk' Ransomware Hackers ...  
forbes.com



have stolen cyberweapons from NSA ...  
techrepublic.com



Your online activity is transparent to ...  
economictimes.indiatimes.com



McAfee: 'Operation Sharpshooter' ha...  
cnn.com



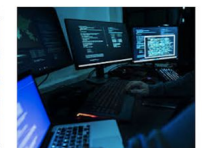
Dear Senior Citizens! You Are an Eas...  
readwrite.com



Hackers for hire – the good, the bad ...  
nakedsecurity.sophos.com



Hacking the Hackers: The French Hacking ...  
fmsh.fr



What Motivates Hackers? | Wald...  
waldenu.edu



Hackers wanted | CSO Online  
csonline.com



Hackers Use Phishing Emails to Harvest ...  
extremetech.com



# What is a hacker?



KubeCon



CloudNativeCon

Europe 2020

*Virtual*

Hacker:  
NOUN

*one who enjoys the intellectual challenge of creatively overcoming limitations.*





KubeCon



CloudNativeCon

Europe 2020

*Virtual*

# How do you work with hackers?



# Crowdsourced Security Testing



KubeCon



CloudNativeCon

Europe 2020

*Virtual*

Vulnerability Coordination	Hacker-Powered Pentests	Bug Bounty Programs
Reactive Approach	Proactive; pay per finding	Proactive: Incentivize research with \$\$\$
See Something? Say Something!	Real-time results	Engineers Learn through Practical Examples
"Welcome Mat"	Diverse testers; results in days	Save \$\$\$ and reduce risk ongoing
Compliance (e.g. ISO 29147)	Compliance; vendor assessments	Cherry on top of the SDLC



KubeCon



CloudNativeCon

Europe 2020

*Virtual*

# Let's get into Kubernetes

# What is the PSC?



KubeCon



CloudNativeCon

Europe 2020

*Virtual*

The Kubernetes Product Security Committee is the one-stop shop for all security-related issues in Kubernetes.

Business-hours on-call rotation by community members.

The active oncall triages incoming security reports:

- From the HackerOne Kubernetes bug bounty program
- From the [security@kubernetes.io](mailto:security@kubernetes.io) mailing list

Valid reports are handled as security incidents.



# Why a BBP for Kubernetes?



KubeCon



CloudNativeCon

Europe 2020

*Virtual*

## First proposal was in February 2018:

- Get more security researcher attention on the Kubernetes codebase
- Simplify triage and response process for the Kubernetes Product Security Committee
- Show that Kubernetes is enterprise-ready
- Widen the net of contributors to Kubernetes security
- Define a way to get security coverage on Kubernetes project infrastructure



KubeCon



CloudNativeCon

Europe 2020

*Virtual*

**A vulnerability is  
submitted. Now what?**

Collapse

## TIMELINE



kebe submitted a report to [Kubernetes](#).

May 7th (3 months ago)

Report Submission Form

### Summary:

Pod files `/etc/hosts`, `/etc/hostname`, `/etc/resolve.conf` are not readonly.  
A normal pod running in kubernetes cluster can kill a host through write data to `/etc/hosts`.  
Not only `/etc/hosts`, but also `/etc/resolve.conf` and `/etc/hostname` can do this.

### Kubernetes Version:

<=1.18

### Component Version:

Docker 19.03

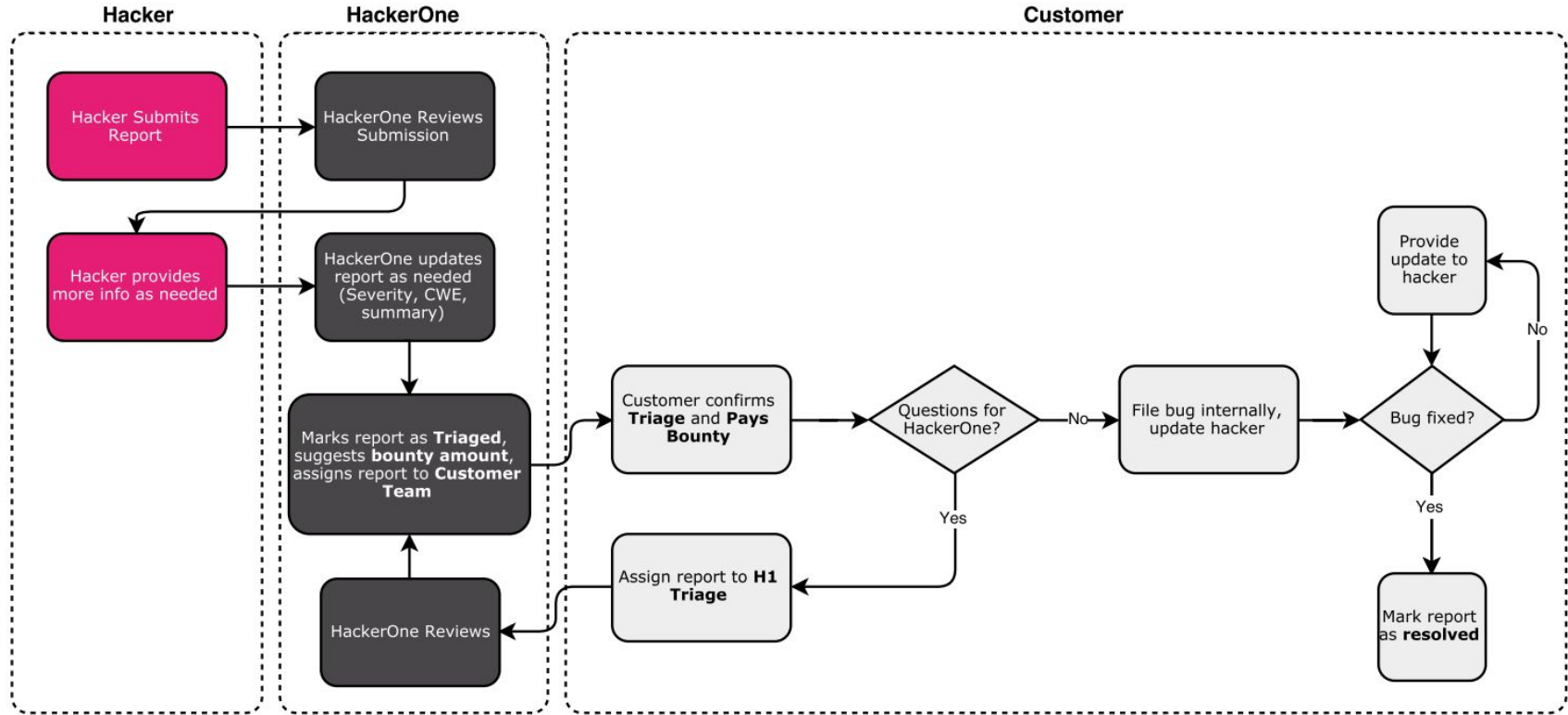
### Steps To Reproduce:

1. use `kubectl` create a pod like `kubectl run`
2. run `kubectl exec -it $POD_NAME -- dd if=/dev/zero of=/etc/hosts count=1000000 bs=10M`
3. run `df -h /var/lib/kubelet` on host that pod running, you can see the disk available space are decreasing until the disk full.

### Supporting Material/References:

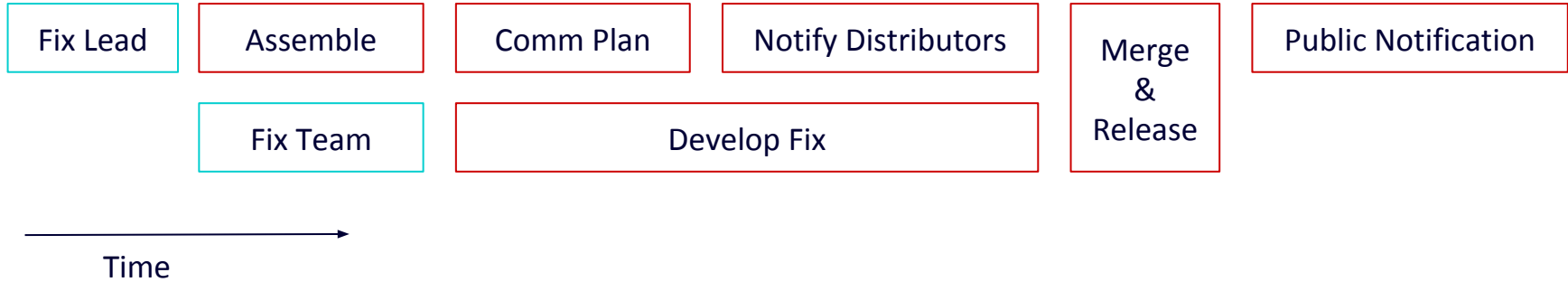
```
[root@kebe-sm-315 ~]# kubectl exec -it rate-c848c5c8b-5b8vm sh
kubectl exec [POD] [COMMAND] is DEPRECATED and will be removed in a future version. Use kubectl kubectl exec
Defaulting container name to rate.
Use 'kubectl describe pod/rate-c848c5c8b-5b8vm -n default' to see all of the containers in this pod.
/ # df -h
Filesystem              Size      Used Available Use% Mounted on
/dev/mapper/docker-8:16-67108930-710df5c781bd17e11968371b9d0f84641a2efde95c68a47eddf9ae518e768d1
10.0G                  40.3M      10.0G      0% /
tmpfs                   64.0M           0    64.0M      0% /dev
tmpfs                    9.7G           0     9.7G      0% /sys/fs/cgroup
/dev/mapper/centos-root
53.0G                  28.6G      24.4G     54% /dev/termination-log
/dev/sdb                100.0G        40.9G     59.1G    41% /etc/resolve.conf
/dev/sdb                100.0G        40.9G     59.1G    41% /etc/hostname
/dev/mapper/centos-root
53.0G                  28.6G      24.4G     54% /etc/hosts
shm                     64.0M         8.0K     64.0M      0% /dev/shm
tmpfs                    9.7G        12.0K     9.7G      0% /var/run/secrets/kubernetes.io/serviceaccount
tmpfs                    9.7G           0     9.7G      0% /proc/acpi
```

# The HackerOne Triage Workflow





# Vuln Report: Passed to PSC



# Success Metrics



Portable, extensible, open-source

BOUNTY TOTAL	INDIVIDUAL BOUNTIES	VALID REPORTS	HACKERS
Total Bounties Paid <b>\$14,850</b>	Top Bounty <b>\$5,000</b>	All-Time <b>80+</b>	Thanked <b>24</b>

*Program launched January 2020*

# Vulnerabilities Found



KubeCon



CloudNativeCon

Europe 2020

*Virtual*

Rate of reports has ticked up since launching the BBP.

Highlights:

**CVE-2020-8557:** (Medium) Pods can DOS the host by filling up /etc/hosts.

**CVE-2020-8559:** (Medium or High) An attacker who can modify kubelet traffic can use a malicious redirect to trick a client into operating on another pod.



KubeCon



CloudNativeCon

Europe 2020

*Virtual*

# How can I contribute?

# Who can contribute?



KubeCon



CloudNativeCon

Europe 2020

*Virtual*

**Anyone can contribute!**

**You don't need to be a security wizard!**

**Security bugs often start as normal bugs.**

**Think it through; if there's a security aspect, then submit it to [hackerone.com/kubernetes](https://hackerone.com/kubernetes)**

# How do I submit?



KubeCon



CloudNativeCon

Europe 2020

Virtual

1

## Asset

Select the attack surface of this issue.

Showing: All Types Type to search

- https://prow.k8s.io  
Domain • Critical • Eligible for bounty
- https://kubernetes.io  
Domain • Critical • Eligible for bounty
- k8s.io  
Domain • Critical • Eligible for bounty
- kubernetes-csi.github.io  
Domain • Critical • Eligible for bounty

Currently selected: None

2

## Weakness

Select the type of the potential issue you have discovered. Can't pick just one? Select the best match or submit a separate report for each distinct weakness.

Showing: All clusters Type to search

- Allocation of Resources Without Limits or Throttling (CWE-770)
- Array Index Underflow (CWE-129)
- Authentication Bypass Using an Alternate Path or Channel (CWE-288)
- Brute Force (CWE-307)
- Buffer Over-read (CWE-126)
- Buffer Under-read (CWE-127)

Currently selected: None

3

## Severity (optional)

Estimate the severity of this issue.

None Low Medium High Critical ⓘ

— OR —

None Low Medium High Critical ⓘ

# What do I get for contributing?



TIER 1 (Core)	TIER 2 (Non-Core)	TIER 3 (Infra & Alpha)
Critical <b>\$10,000</b>	Critical <b>\$5,000</b>	Critical <b>\$2,500</b>
High <b>\$5,000</b>	High <b>\$2,500</b>	High <b>\$1,250</b>
Medium <b>\$1,000</b>	Medium <b>\$500</b>	Medium <b>\$250</b>
Low <b>\$200</b>	Low <b>\$100</b>	Low <b>\$100</b>



# How can I stay up to date?



KubeCon



CloudNativeCon

Europe 2020

*Virtual*

**Kubernetes security announcements go to most channels.**

**For focused security announcements:**

**[kubernetes-security-announce@googlegroups.com](mailto:kubernetes-security-announce@googlegroups.com)**

# What's to come for contributors?



KubeCon



CloudNativeCon

Europe 2020

*Virtual*

**SIG Security is in the works.**

**A permanent home for the work done by the PSC.**

**You can join in the discussion and help establish processes for the new SIG.**

**Follow the discussion with [SIG Auth](#) and**

**[kubernetes-security-discuss@googlegroups.com](mailto:kubernetes-security-discuss@googlegroups.com)**



KubeCon



CloudNativeCon

Europe 2020



HELM

*Virtual*



KEEP CLOUD NATIVE

CONNECTED

