



Forget Everything You Know About Image Vulnerability and Prioritization

Oshrat Nir & Ben Hirschberg
ARMO



Are you in
CVE Shock?



I DON'T KNOW

WHAT IS CVE SHOCK?



Leo Di Donato
@leodido · [Follow](#)



CVE shock.

The state of total helplessness when facing the overwhelming list of CVEs returned by the vulnerability scanners.

3:11 PM · Jul 19, 2022



[Read the full conversation on Twitter](#)



11



Reply



Share

[Read 2 replies](#)



/whoami

- > Ben Hirschberg
- > Co-founder && CTO @ARMO
- > Kubescape maintainer
- > Whitehat in the past (unofficially still ;-)
- > Fluent in Hebrew, Hungarian, C, ASM and Go (not English)
- > Contributor in CNCF-WG + organizer of CNCF Jerusalem
- > Father of 4 <3



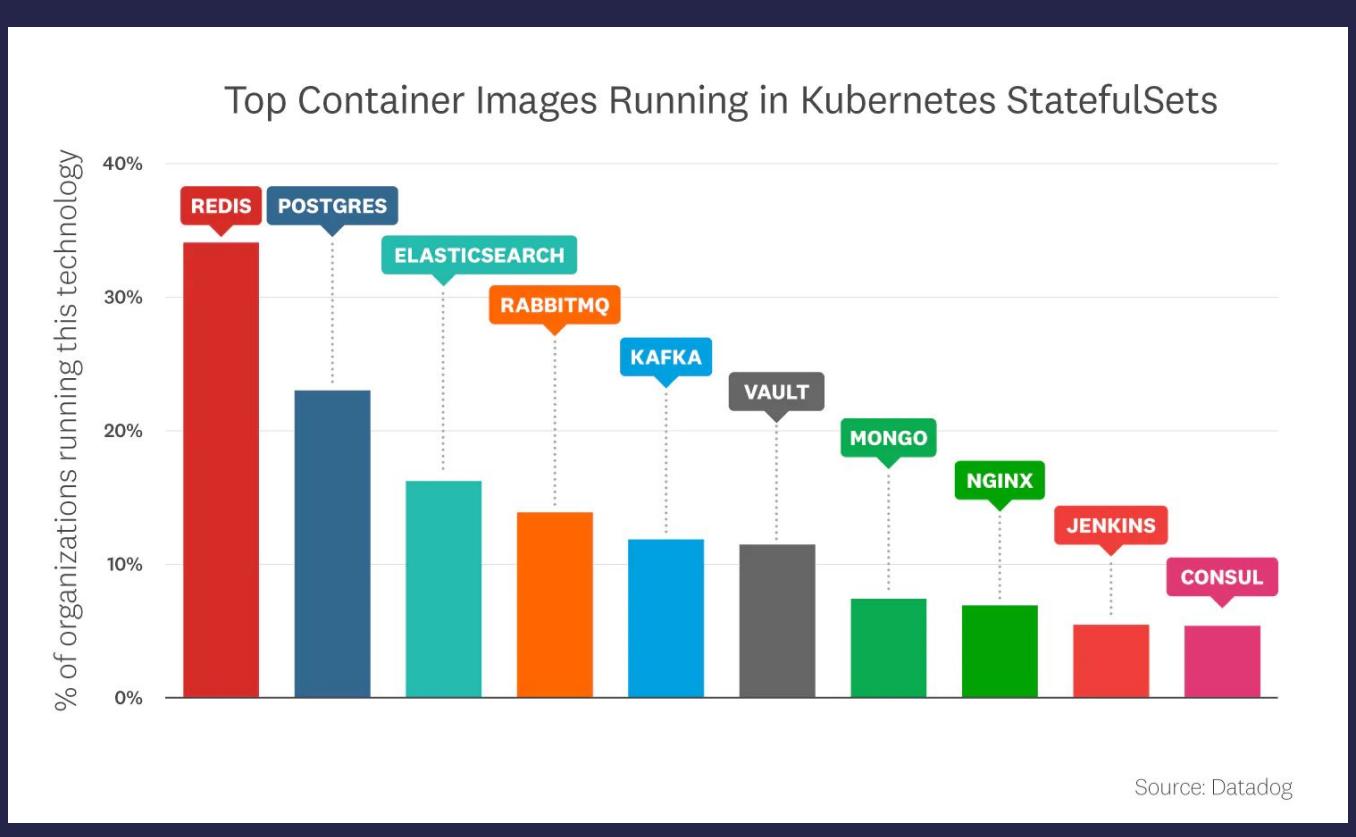
#Ben Hirschberg

-  linkedin.com/in/ben-hirschberg
-  [@slashben81](https://twitter.com/slashben81)
-  github.com/slashben

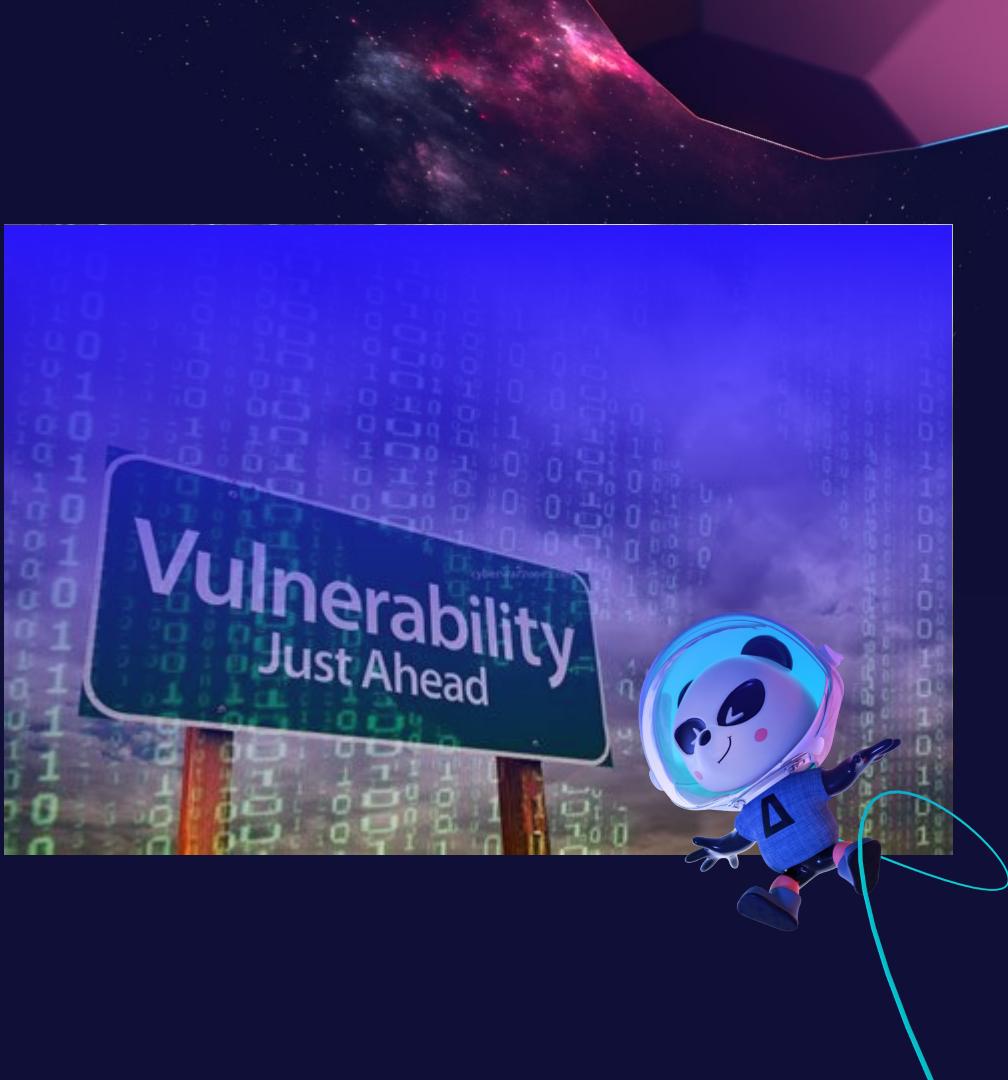
Where are you
looking for CVEs?



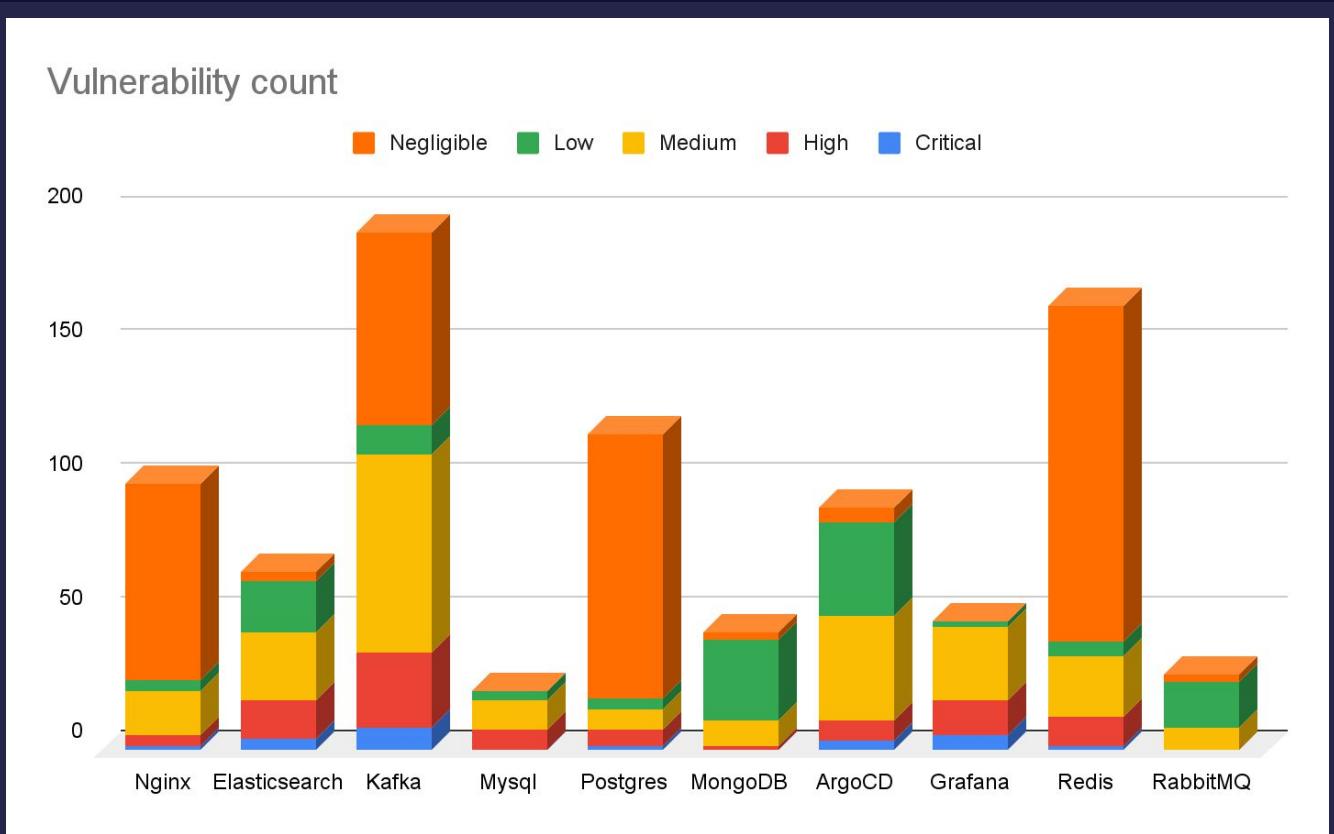
/Everybody use public images_



**Unfortunately,
they come with many
vulnerabilities**



/Vulnerabilities in common images_



/Where are you looking for CVEs?_

Container
Registry

CI/CD

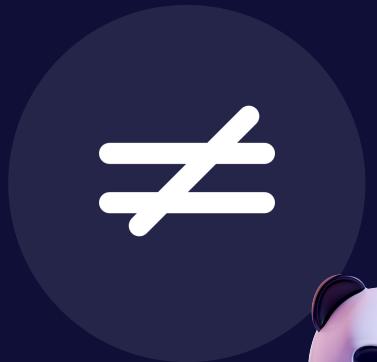
Cluster

Container
Images



/Reality_

Vulnerability
in image



Workload
exploit

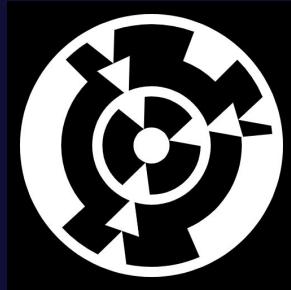


/Let's put things in CONTEXT_



Reachability

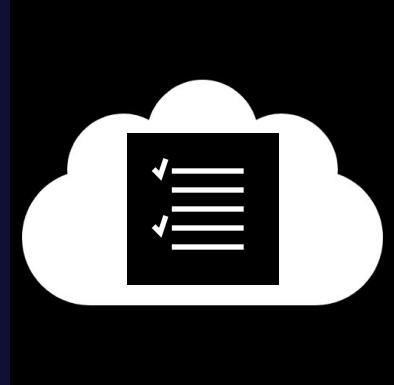
Asset
Criticality



Provenance



Threat
Intelligence



Prioritized
Vulnerability



/Introducing CVSS

Common Vulnerability Scoring System - an open industry

- standard for assessing the severity of computer system security vulnerabilities

Used to prioritize the response to security incidents and to calculate the potential impact of incidents

- Widely adopted, yet lacks context



/Introducing KEV_

- **KEV - A CISA maintained list of Known Exploited Vulnerabilities**
- Vulnerabilities posing increased risk because they are being actively exploited
- Required as part of a complete vulnerability management strategy



/KEV_coverage_



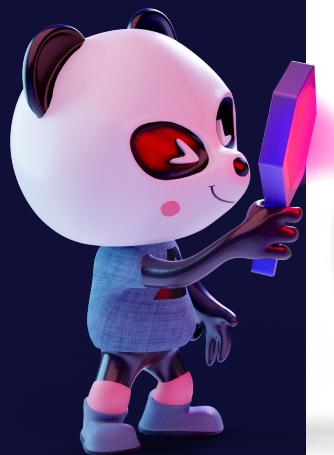
Total	P0 (KEV)
23,082	41
14,075	39
19,030	34
31,535	35
6,586	15

/Introducing EPSS

- A machine learning based model that assess the likelihood of a vulnerability being exploited in the future
- Analyzes factors associated with vulnerabilities, such as its characteristics, historical exploit data, etc.
- Indicates the probability of a vulnerability being targeted by attackers within the next 30 days



/Proving the point with EPSS_



EPSS Comparison by Coverage

By matching the coverage across three different prioritization scores, we can compare the savings in effort and efficiency of that effort.

CVSS v3

Threshold: 8.8+
Effort: 253/1000
Coverage: 50.7%
Efficiency: 5.0%

EPSS v1

Threshold: 0.066+
Effort: 93/1000
Coverage: 51.2%
Efficiency: 12.9%

EPSS v2

Threshold: 0.149+
Effort: 47/1000
Coverage: 50.9%
Efficiency: 42.5%

All CVEs Remediated Exploited

Scored 2021-11-01, compared against exploitation activity in following 30 days

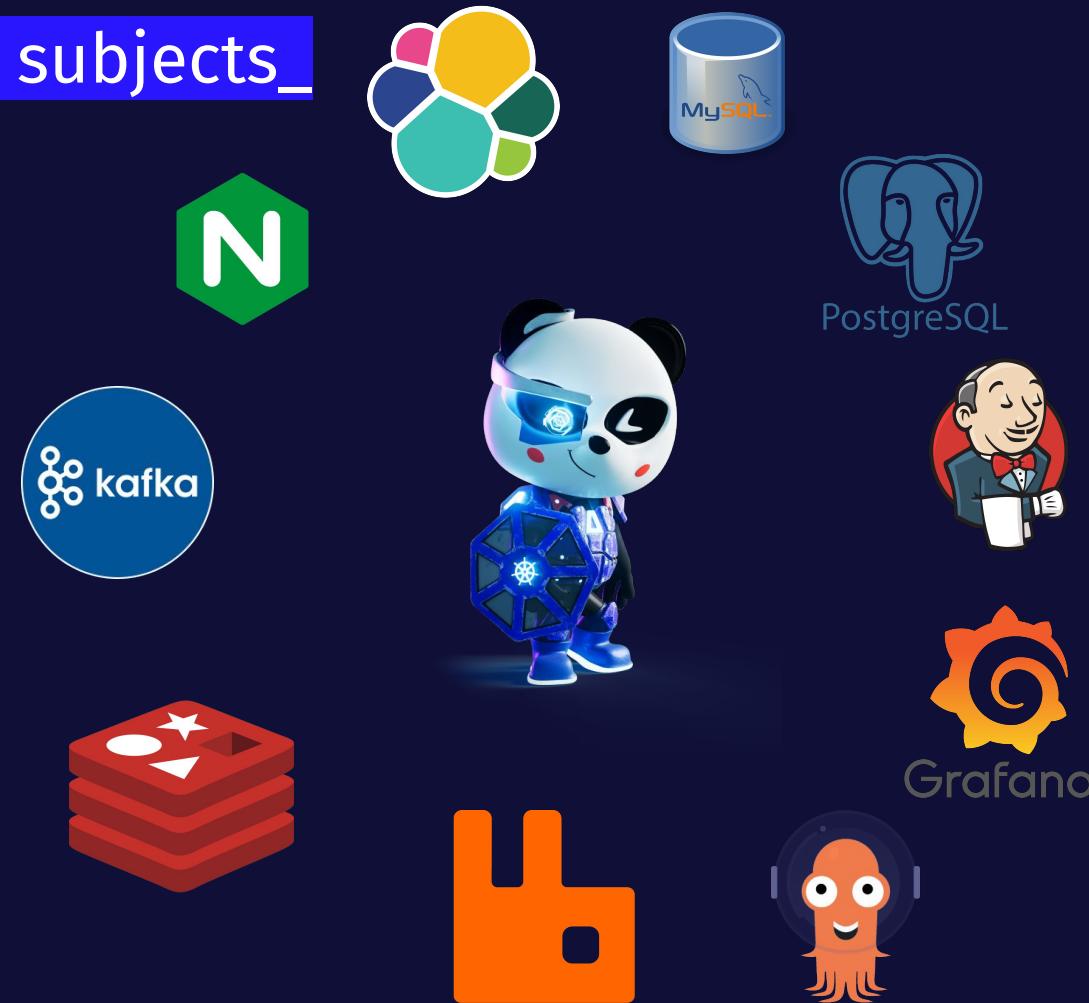
Image source: www.first.org

/Introducing Reachability_

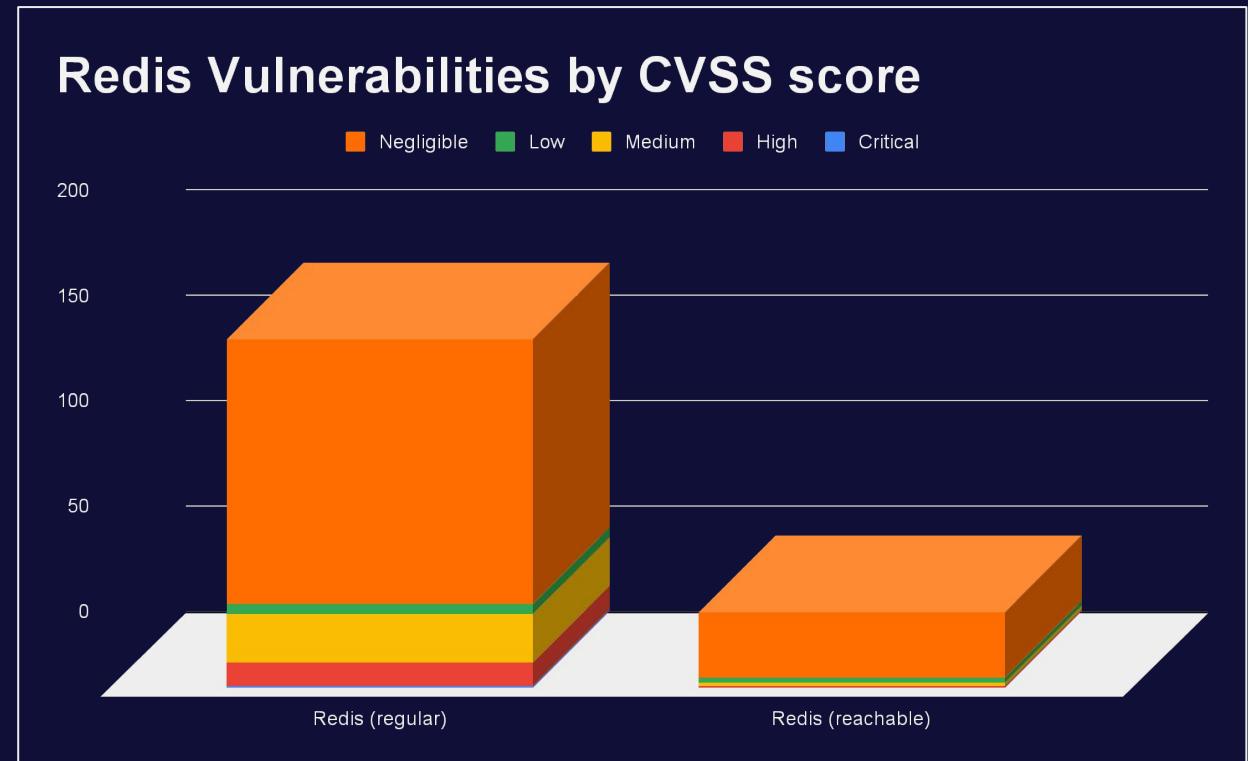
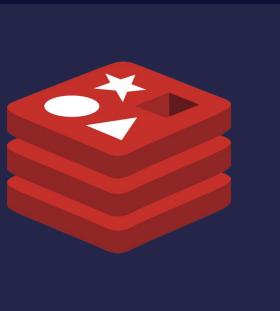
- AKA “Relevancy”
- Vulnerable software component is loaded into the memory
- Not loaded, cannot be exploited

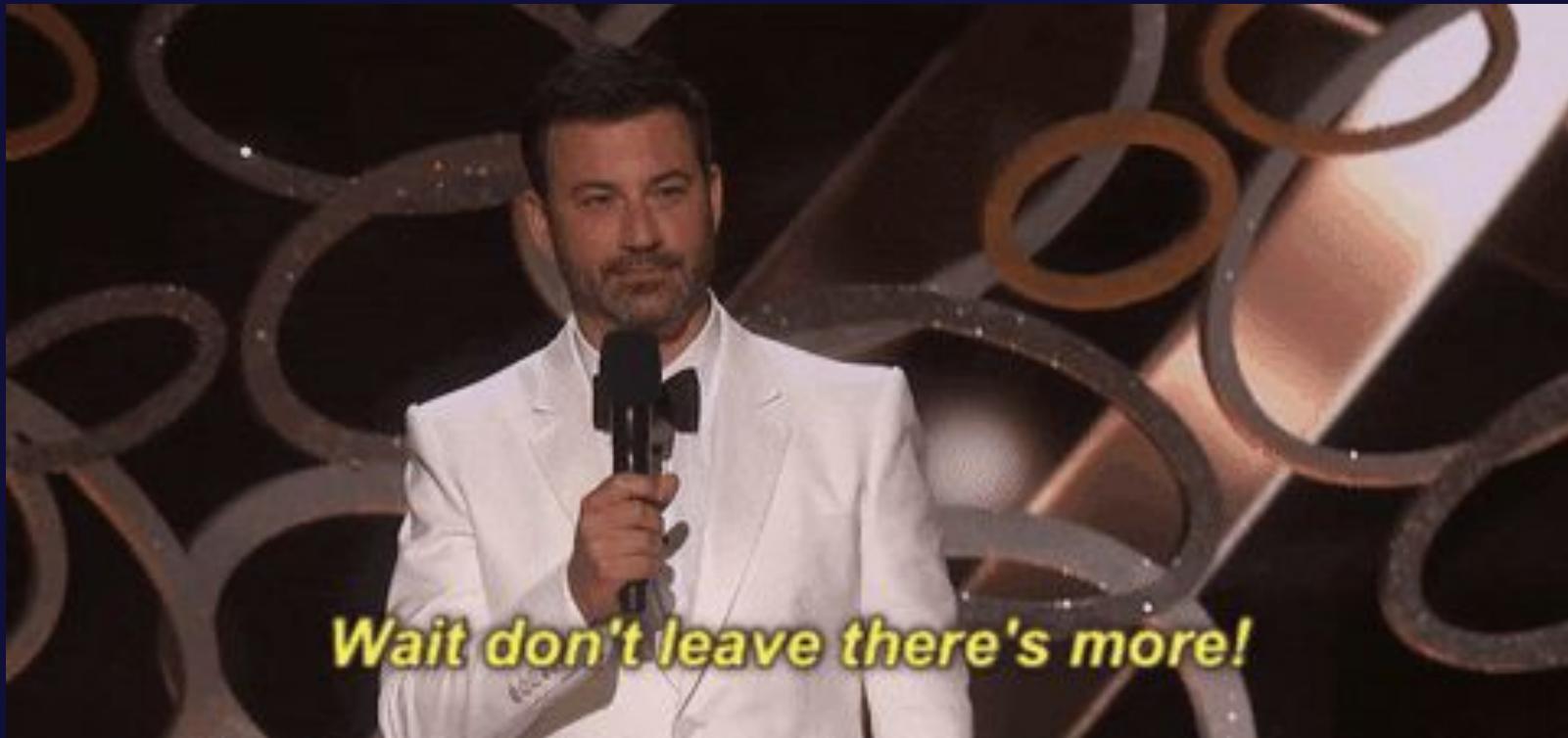


/Research subjects_



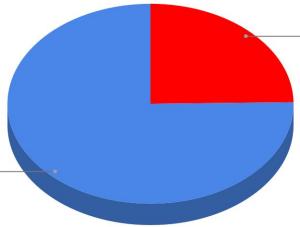
/Consider Redis_



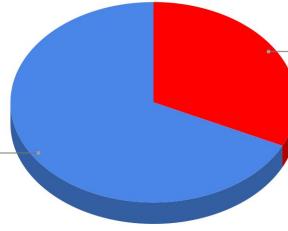


Wait don't leave there's more!

/Additional results_



Only 25%
reachable CVEs

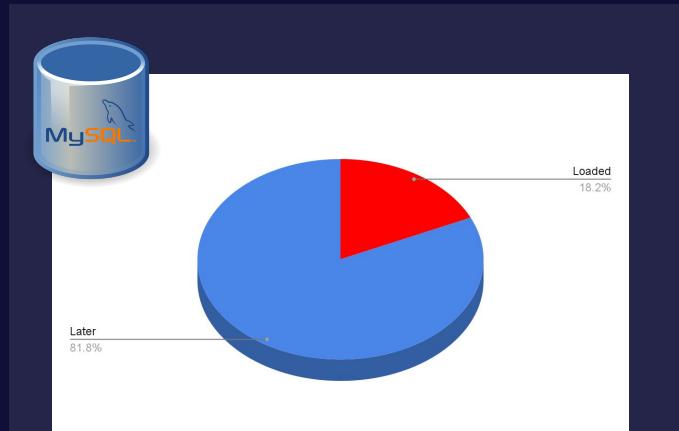


Less than a third
reachable CVEs

/Additional results_



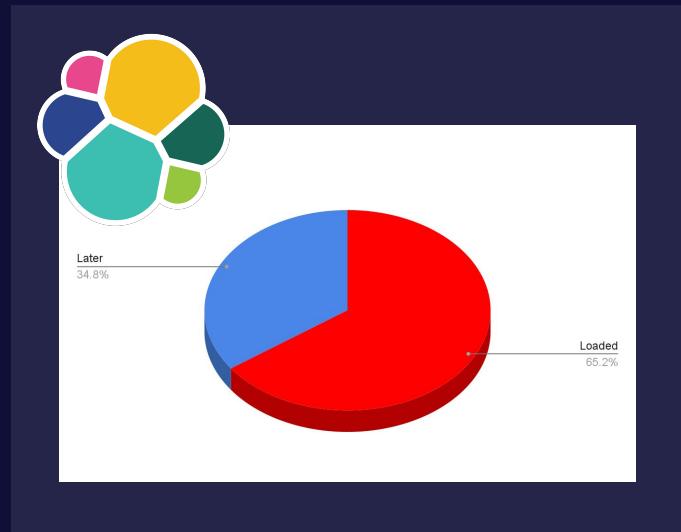
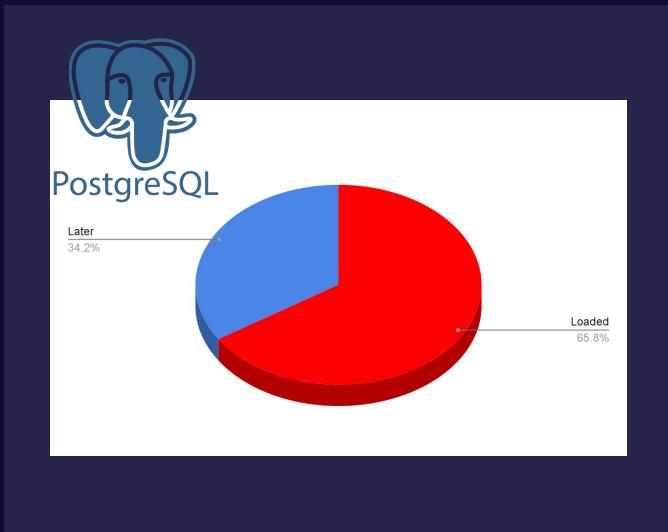
Less than half
reachable CVEs



Less than 20%
reachable CVEs

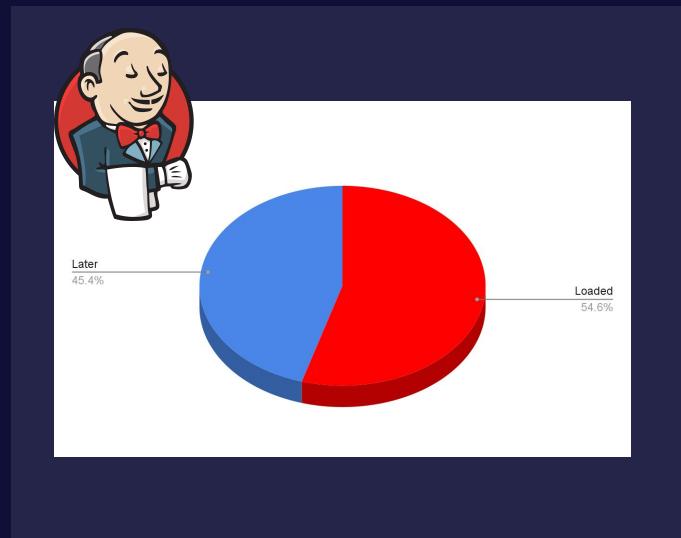
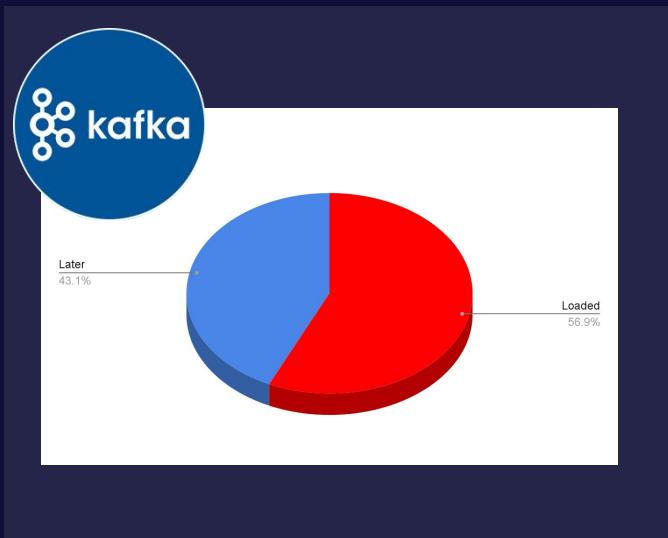


/Additional results_



Less than 2/3 reachable CVEs

/Additional results_



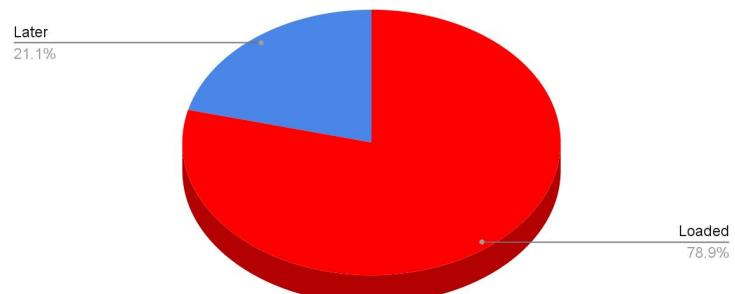
Less than 60% reachable CVEs

/The case of Grafana_



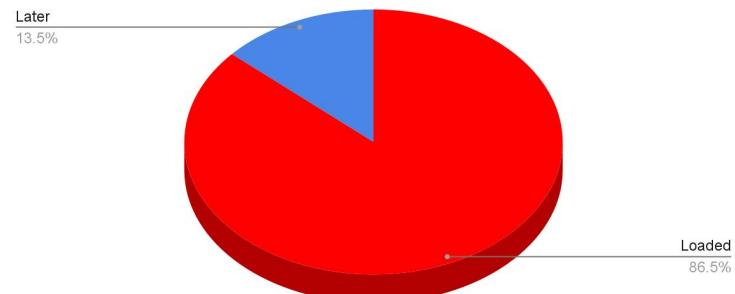
Grafana

Grafana 9.0.4



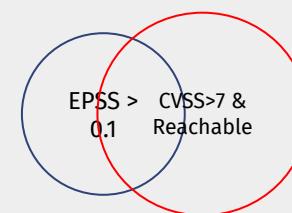
May

Grafana 10.1.2



October

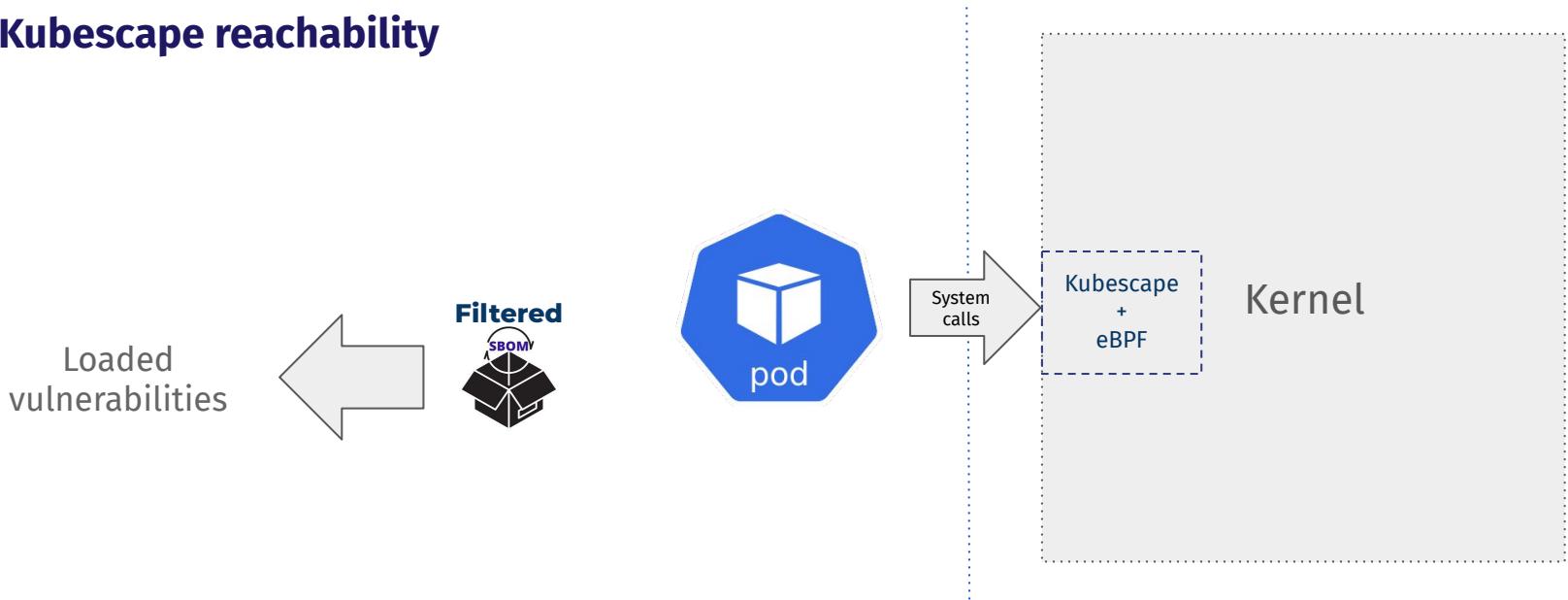
/Reachability_n_EPSS_



48% of EPSS>0.1 not reachable



Kubescape reachability



/ARMO platform (powered by Kubescape) > Relevant CVEs

ARMO
POWERED BY KUBESCAPE

Talk to an Expert

ARMO Platform Team J

Vulnerabilities

TOTAL VULNERABILITIES **3,918**
2,151 Fixable
254 RCE
668 Relevant

Critical **169**
157 Fixable
61 RCE
50 Relevant

High **875**
673 Fixable
98 RCE
173 Relevant

Medium **1,384**
1,114 Fixable
67 RCE
238 Relevant

Low **211**
131 Fixable
8 RCE
22 Relevant

Negligible **1,233**
69 Fixable
20 RCE
175 Relevant

Unknown **46**
7 Fixable
0 RCE
10 Relevant

668 vulnerabilities were found relevant [Learn more](#)

Vulnerabilities over time

Last 6 Weeks

● Critical 169 ● High 875 ● Medium 1384 ● Low 211 ● Negligible 1233 ● Unknown 46

Search CVE Scan time: 29/10/2023 - 30/10/2023 Fixable: Yes Relevant: (2) + Add filter Clear all filters [Feedback](#)

STAT.	SCAN TIME	CLUSTER	NAMESPACE	WORKLOAD	CONTAINER NAME	REGISTRY	IMAGE TAG	RELEVANT	SEVERITY	0	2	3	0	0	0
Oct 30, 2023 09:52:19		armo-platform-cluster	kubescape	daemonset-host-scanner	host-sensor	quay.io	quay.io/kubescape/host-scanner:v1.0.66	N/A		0	2	3	0	0	0
Oct 30, 2023 08:44:02		armo-platform-cluster	kubescape	deployment-otel-collector	otel-collector	docker.io	docker.io/otel/opentelemetry-collector:0.86.0	N/A		0	1	3	0	0	0
Oct 30, 2023 08:44:01		armo-platform-cluster	default	deployment-internal-proxy-deployment	info-app	docker.io	docker.io/madhukarula/k8s-goat-info-app	35		5	33	19	1	0	0
Oct 30, 2023 08:44:00		armo-platform-cluster	default	deployment-internal-proxy-deployment	internal-api	docker.io	docker.io/madhukarula/k8s-goat-internal-api	26		15	45	46	6	0	0
Oct 30, 2023		armo-platform-	kubescape	deployment-gateway	gateway	quay.io	quay.io/kubescape/gate	N/A		0	1	2	0	0	0

/Conclusion_

- **Using public images exposes you to vulnerabilities**
- **The results of vulnerability scans may cause CVE Shock**
- **Reachable vulnerabilities point to the small subset that should be addressed first**



ΔRMO

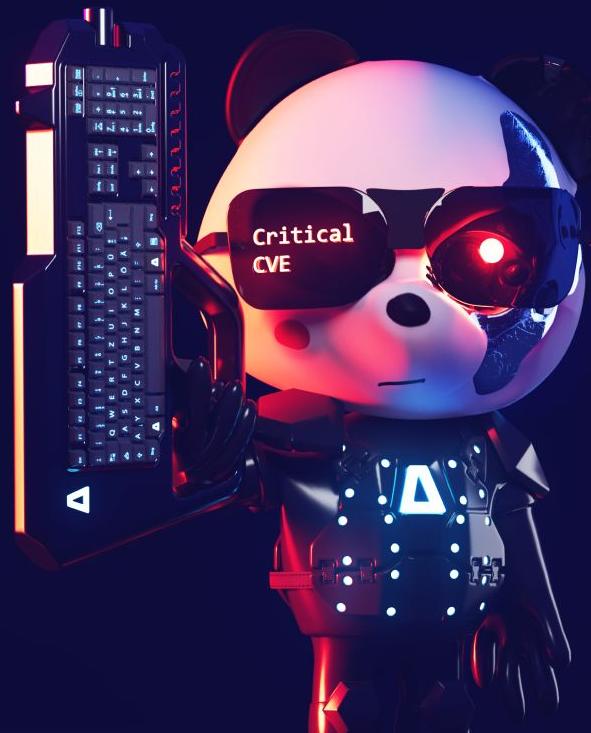
The Makers of Kubescape 

Interested in becoming
a K8s CVE terminator?

Come and meet us at
ARMO booth F12

There's cool swag
waiting for you...

Hasta la vista, CVE



_Terminate your
most relevant
CVEs, now />



Thank you_



ΔRMO

