
KubeCon
CloudNativeCon
North America 2023


KubeCon | CloudNativeCon

North America 2023

SIG Security: Unravelling the Kubernetes Security Audit Together

Ala Dewberry, VMware
Pushkar Joglekar, Independent
Rey Lejano, SUSE
Savitha Raghunathan, Red Hat

What is SIG Security?

- Horizontal SIG that covers security initiatives for the entire Kubernetes project
- Open, community based approach
- Core Services include:
  - Self Assessments
  - Docs
  - Tooling
  - Third Party Audit
- Come make good trouble!
  - #sig-security
  - Join the Google Group

SIG Security - Assessments Subproject

Who are we and what do we do?

- Threat modeling subproject
- Output: threat models for different pieces of Kubernetes
- Outcome: Secure Kubernetes by making threat modeling a community norm

SIG Security - Assessments Subproject

What are we up to?

- vSphere CSI Driver Self Assessment
- Sequence/Component Diagrams are complete
- Now for the fun - STRIDE model!

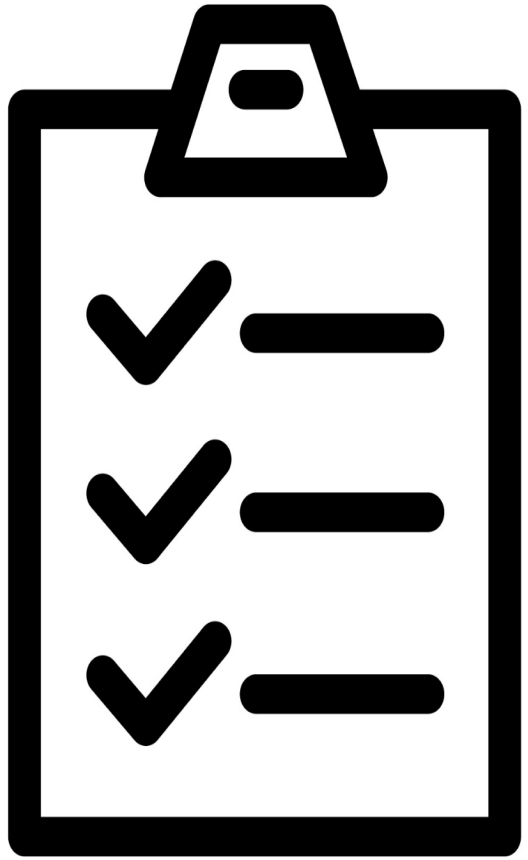
kubernetes-sigs/**vsphere-csi-driver**

vSphere storage Container Storage Interface (CSI) plugin

SIG Security - Assessments Subproject

High Level Threat Modeling Process

- Find your people
- Map the attack surface - Draw Sequence/Component Diagrams
- Conduct the assessment
- Write it up
- Review Process
- Completion!



SIG Security - Assessments Subproject

How can you get involved?

- Slack channels:
  - #sig-security-assess-vsphere-csi-driver
  - #sig-security-assessments
  - DM Ala Dewberry
- Help out with the STRIDE model for the vSphere CSI Driver
- Suggest our next assessment target!

SIG Security - Docs Subproject

- Sub Project Goals:

  - Collaborate and create/improve existing security content for Kubernetes documentation.
  - Keep the documentation and security examples up to date.
  - Create security awareness through documentation.

- Current Projects:

  - Hardening guide
    - Authentication Mechanisms
    - RBAC - WIP

SIG Security - Docs Subproject

- Future Projects:

  - Update Kubernetes security checklist application deployment.
  - Kubernetes RBAC guide and tutorial.

- sig-security-docs subproject is looking for volunteers!

- If you have an idea to improve the security content of Kubernetes website, please feel free to start a thread in the slack channel and/or create an issue in the k/website repo.

SIG Security - Tooling Subproject

- We write *code* to Make Kubernetes *more* Secure

Vulnerability Scanning

- Scans go modules of k/k
- Scans container release images
- Scans every 6 hours for last 2+ years

Co-maintainers:

- SIG Architecture
- SIG Release
- SIG Testing
- SIG K8s Infra

Official CVE Feed

- Publicly announced CVEs
- Auto-refreshing
- Alpha (v1.25) → Beta (v1.27) → GA *soon*!

Co-maintainers:

- Security Response Committee
- SIG Docs
- SIG Testing
- SIG K8s Infra

SIG Security - External Audit Subproject

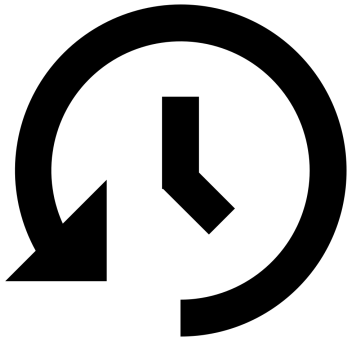
We coordinate regular, comprehensive, third-party security audits

External Audit Subproject Goals:

- Identify vulnerabilities or weaknesses in Kubernetes
- Make Kubernetes more secure

Started as WG Security Audit

SIG Security - 2019 Audit



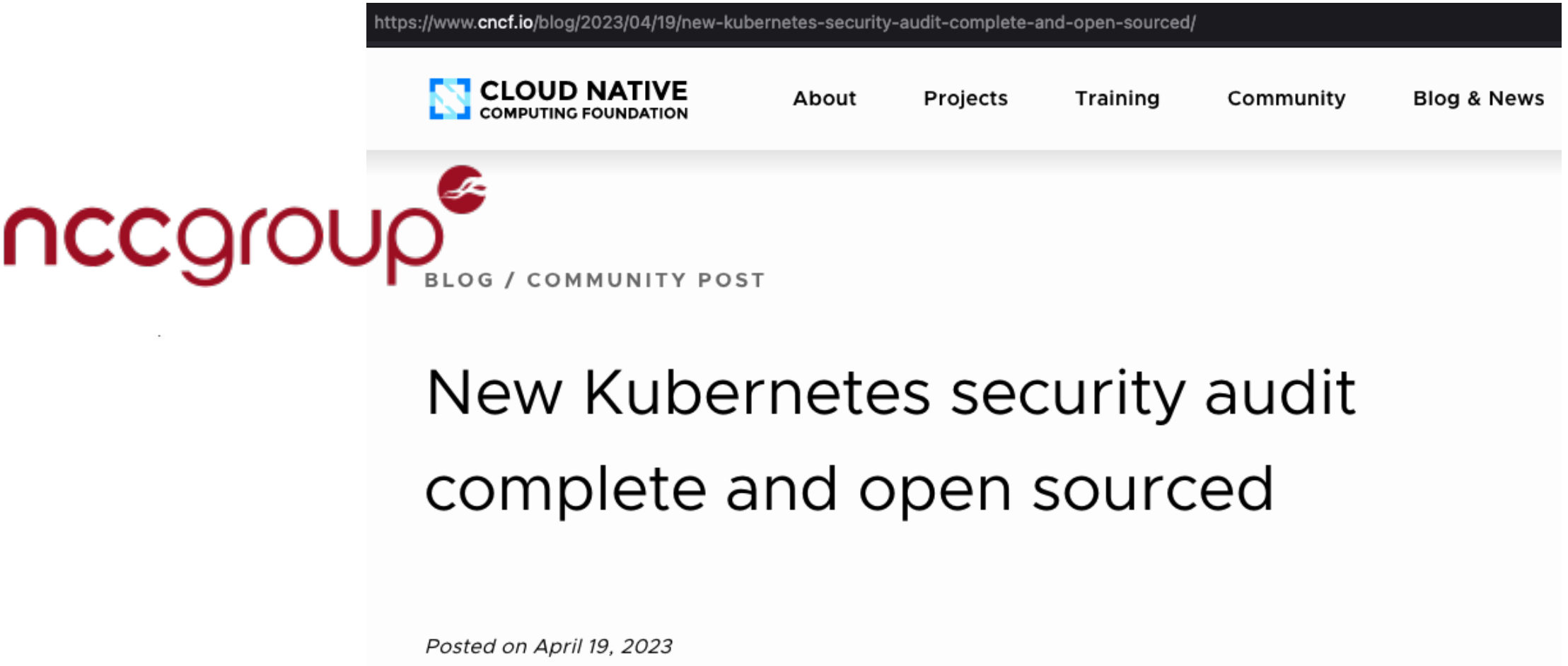
First external security audit was published in 2019
https://github.com/kubernetes/sig-security/blob/main/sig-security-external-audit/security-audit-2019/findings/Kubernetes%20Final%20Report.pdf

Based on Kubernetes 1.13.4

Last year, blog published as a retrospective on the current state 2019

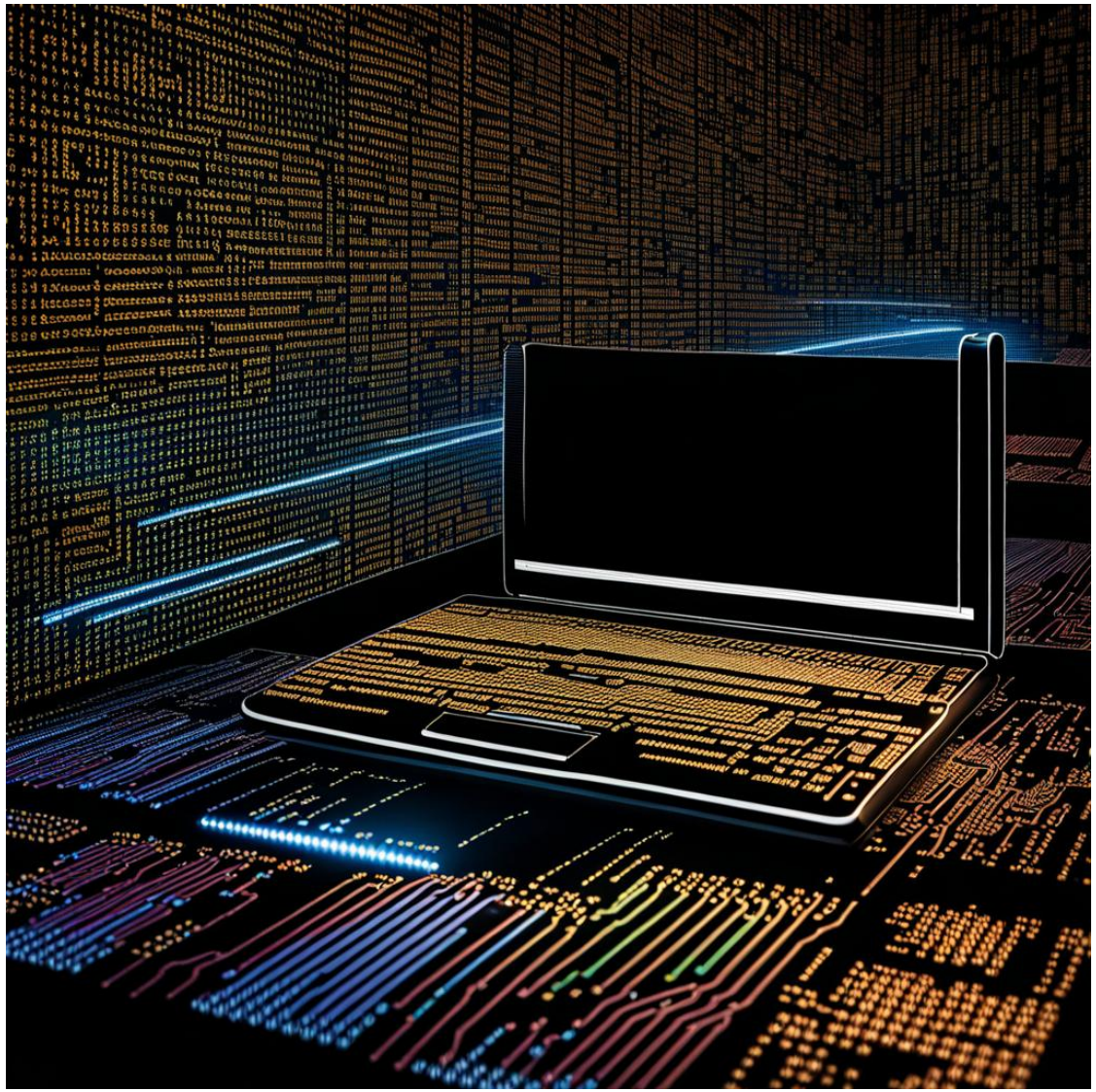
- https://kubernetes.io/blog/2022/10/05/current-state-2019-third-party-audit/
- Reviews the status of the 37 issues filed from the 2019 audit
  - 21 fixed
  - 5 needs a KEP

Kubernetes Security Audit



https://github.com/kubernetes/sig-security/blob/main/sig-security-external-audit/security-audit-2021-2022/findings/Kubernetes%20v1.24%20Final%20Report.pdf

Kubernetes Security Audit



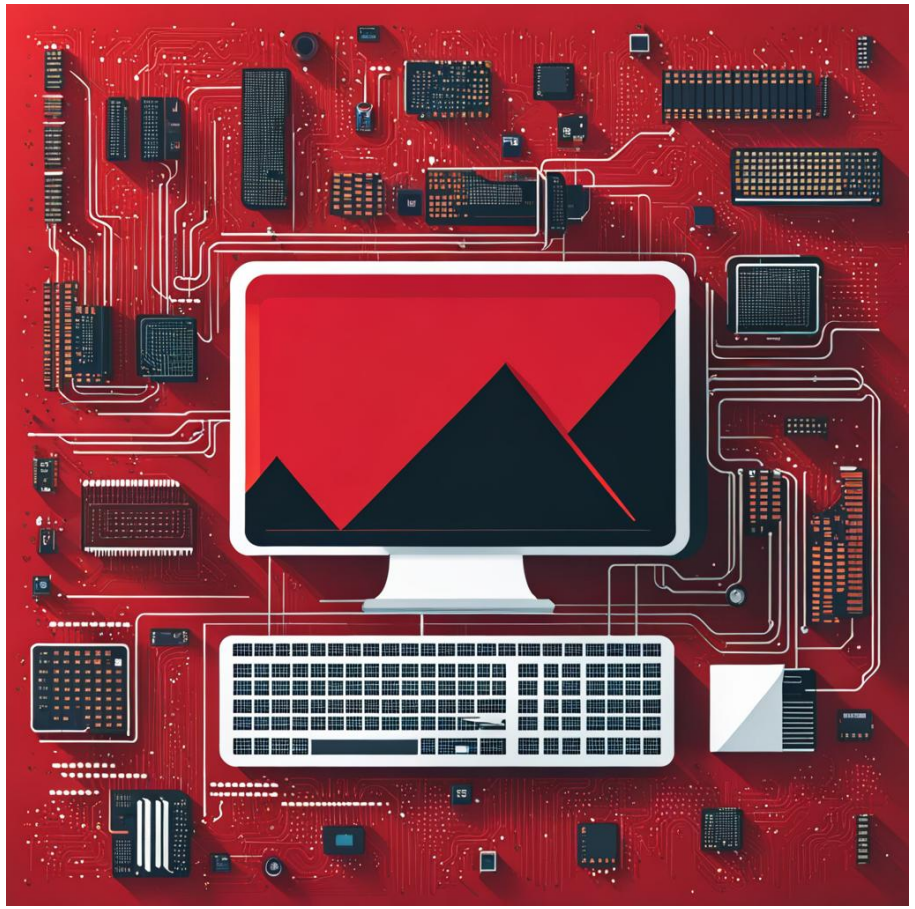
Audit based on Kubernetes 1.24

Scope:

- kube-apiserver
- kube-scheduler
- Kubernetes use of etcd
- kube-controller-manager
- cloud-controller-manager
- kubelet
- kube-proxy
- secrets-store-csi-driver

Kubernetes Security Audit

19 findings
Umbrella issue in GitHub kubernetes/kubernetes
https://github.com/kubernetes/kubernetes/issues/118980



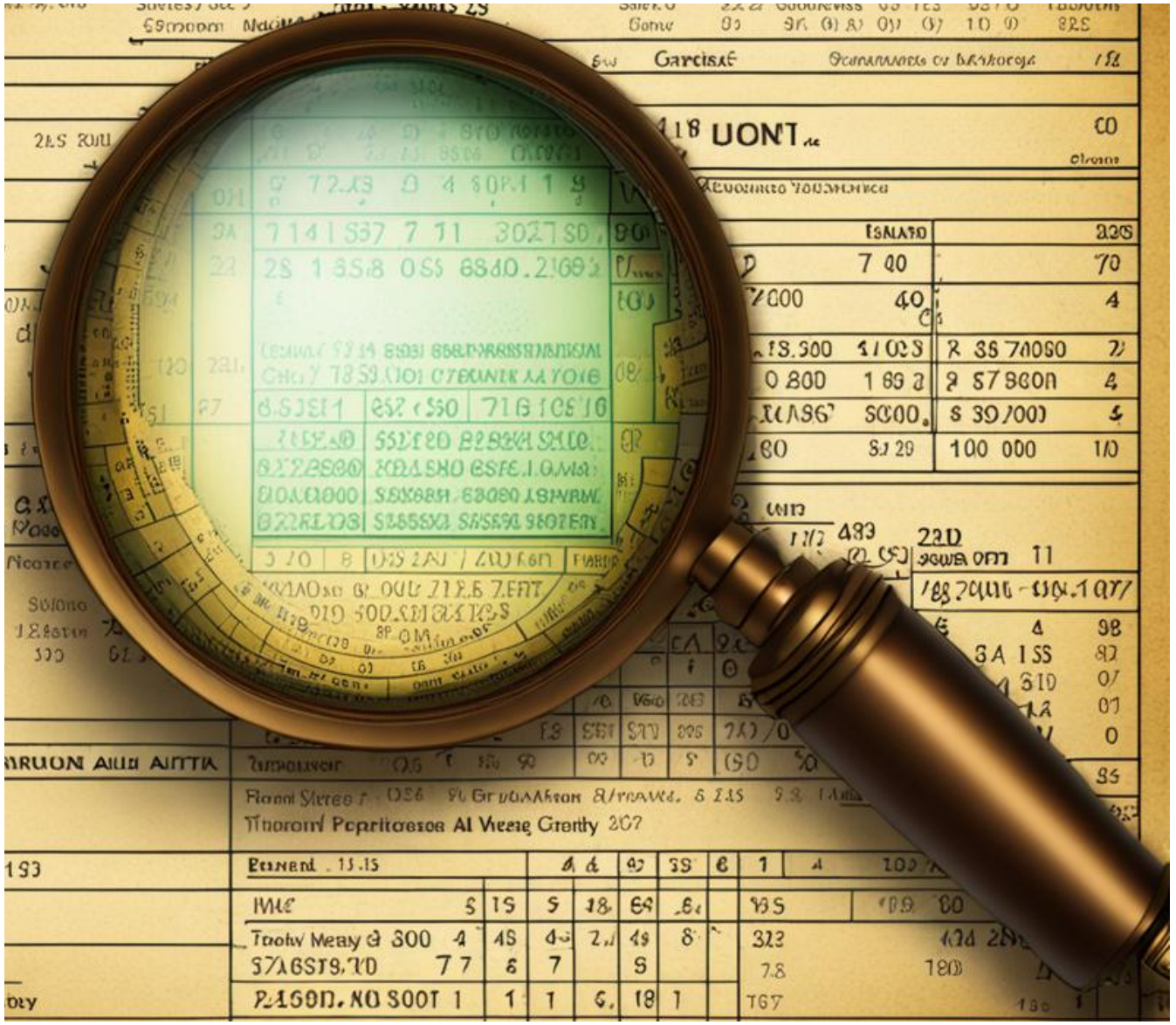
#	Title	Issue	Status
1	Additive Access Controls	#118982	
2	Multiple Concerns with Network Policies	#118983	wontfix
3	Lack of Cohesion Between Core Access Control Mechanisms	#118985	
4	Weaknesses in Pod Security Standards Restricted Profile	#118987	
5	Common Certificate Authority Possible for Client CA and Request Header CA	#119267	
6	Path Traversal in Namespace Specifier	#119269	fixed
7	Redirection of API Server Traffic to Kubelet	#119270	
8	API Server Proxy Disables TLS Certificate Validation	#119625	
9	Authentication Source Not Shown in Audit Logs	#119626	
10	EmptyDir Volumes Do Not Support Mount Options	#119627	
11	Loopback Token Usable Externally	#119628	
12	Inaccurate X-Forwarded-Uri Header	#119629	
13	Logging of Incorrect Bootstrap Tokens	#119630	fixed
14	Incorrect Handling of Proxy Authentication Headers	#119631	fixed
15	Timing Side Channel in Bootstrap Tokens Generation and Handling	#119632	
16	Non Constant-Time Comparison of Service Account Token Secrets	#119638	not a security issue, but fixed
17	Low Entropy Bootstrap Tokens	#119639	needs KEP
18	Privilege Escalation via `nodes/proxy` Permission	#119640	
19	Dangerous File Path Construction	#119641	

Kubernetes Security Audit Breakdown

Category	# of Findings
Access Controls	7
Authentication	4
Configuration	1
Cryptography	4
Data Validation	1

Risk Level	# of Findings
Critical	0
High	0
Medium	6
Low	9
Informational	4

Component	# of Findings
Security Architecture Review	4
kube-apiserver	13
kubelet	2

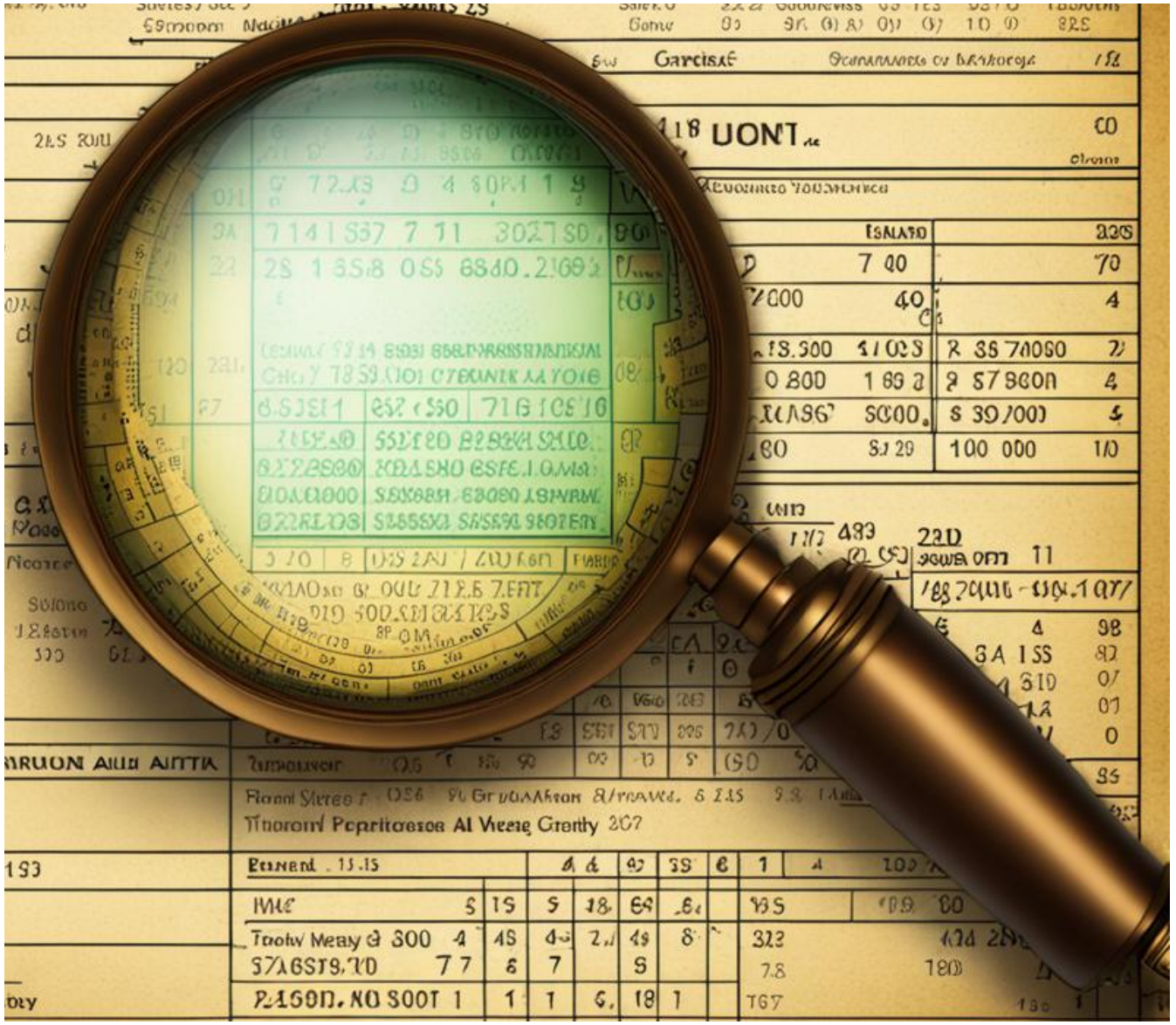


Kubernetes Security Audit Breakdown

Category	# of Findings
Access Controls	7
Authentication	4
Configuration	1
Cryptography	4
Data Validation	1

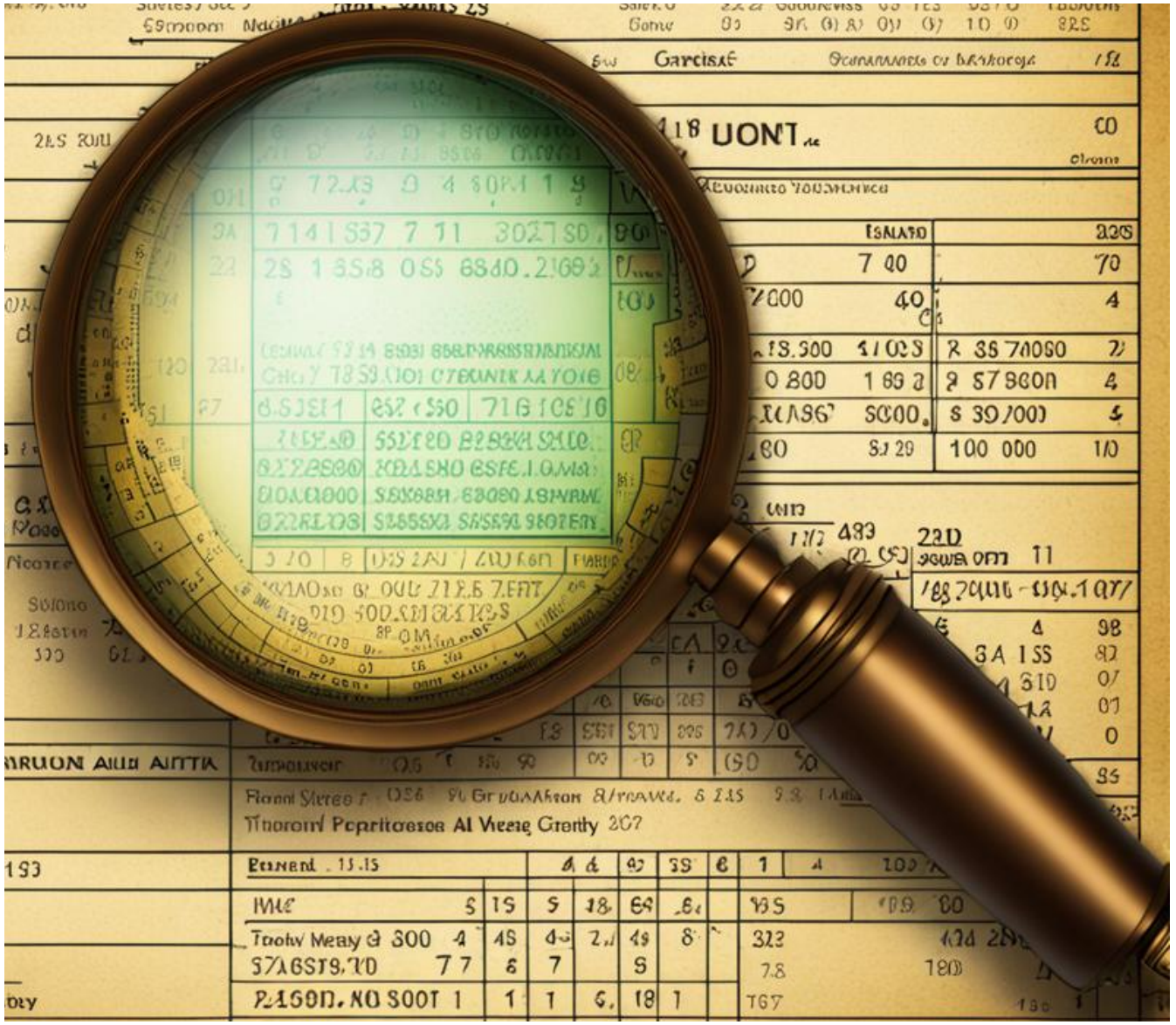
Risk Level	# of Findings
Critical	0
High	0
Medium	6
Low	9
Informational	4

Component	# of Findings
Security Architecture Review	4
kube-apiserver	13
kubelet	2



Kubernetes Security Audit Breakdown

Risk Level	# of Findings
Critical	0
High	0
Medium	6
Low	9
Informational	4



Kubernetes Security Audit
Medium Risk

Risk Level	# of Findings
Critical	0
High	0
Medium	6
Low	9
Informational	4

Category	# of Medium Findings
Access Controls	3
Authentication	2
Cryptography	1

Component	# of Medium Findings
Security Architecture Review	1
kube-apiserver	4
kubelet	1

Medium Risk Findings

Additive Access Controls

Component: Security Architecture Review
Category: Access Control

Authorization in Kubernetes is mostly handled by RBAC.
“Permissions are purely additive (there are no "deny" rules)”
– kubernetes.io

Recommendation is to enhance RBAC to support explicit “deny” rules that return DecisionDeny

Medium Risk Findings

Common Certificate Authority Possible for Client CA and Request Header CA

Component: kube-apiserver
Category: authentication

Medium Risk Findings

Path Traversal in Namespace Specifier

Component: kube-apiserver
Category: Access Controls

Users can bypass access controls by passing directory traversal sequence (..) to the Kubernetes API. Therefore users can find the full path of objects they should not have access to.

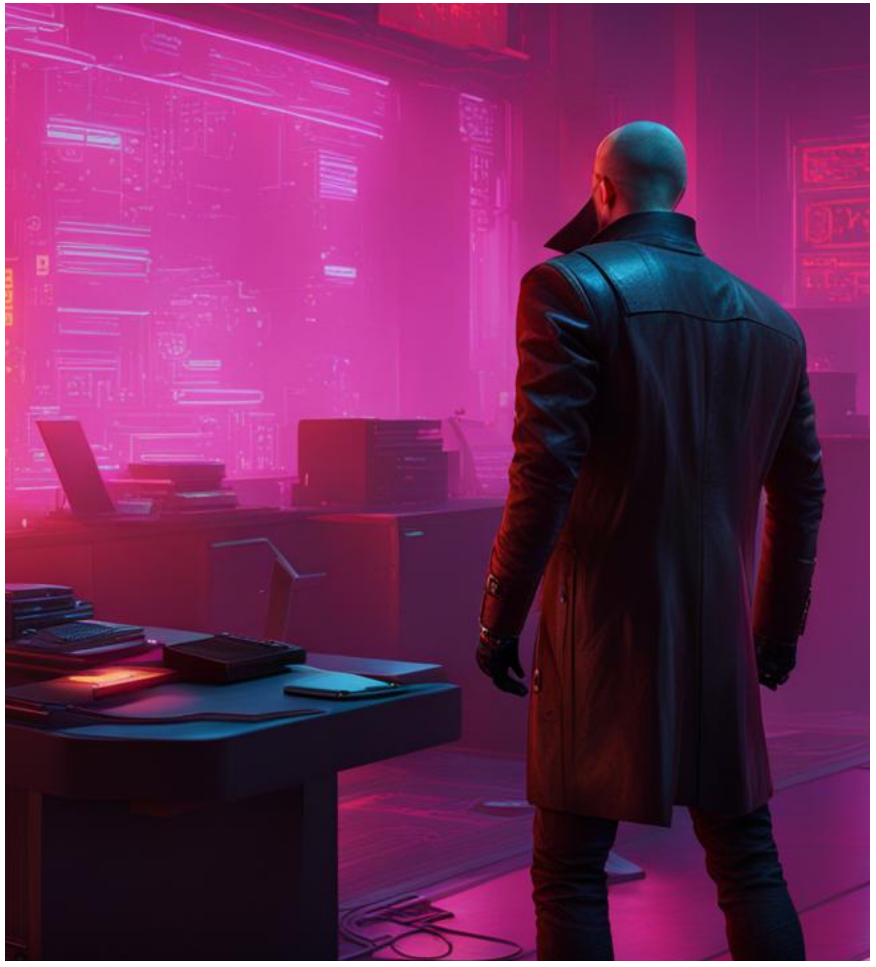
Recommendation is to add a check on namespace identifier in API requests.

Medium Risk Findings

Redirection of API Server Traffic to Kubelet (privilege escalation)

Component: kube-apiserver (proxy)

Category: Authentication



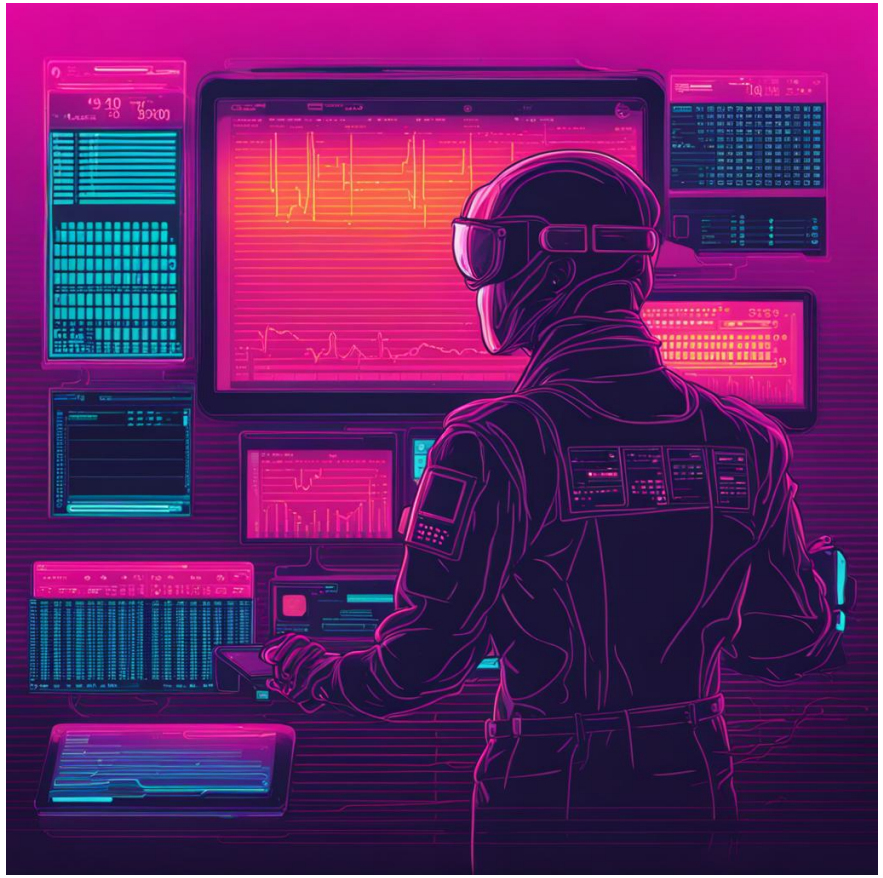
Medium Risk Findings

API Server Proxy Disables TLS Certificate Validation

Component: kube-apiserver (proxy)
Category: Cryptography

Someone can intercept TLS connections from the API server proxy to Pods, Services, or Nodes (not from the client to the API Server) and read or modify.

Recommendation is to implement TLS certificate validation for Pod, Service, Node proxying.



Medium Risk Findings

Audit Roadmap

The audit roadmap lists previously audited focus areas and focus areas requested to be included in future audits.

kube-state-metrics	TBD	https://github.com/kubernetes/kube-state-metrics
node feature discovery	TBD	https://github.com/kubernetes-sigs/node-feature-discovery
hierarchial namespace	TBD	https://github.com/kubernetes-sigs/multi-tenancy/tree/master/incubator/hnc
pod security policy replacement	TBD	https://github.com/kubernetes/enhancements/tree/master/keps/sig-auth/2579-psp-replacement
CoreDNS (in the context of Kubernetes use of CoreDNS)	TBD	Concept: https://kubernetes.io/docs/concepts/services-networking/dns-pod-service/ Reference: https://kubernetes.io/docs/tasks/administer-cluster/dns-custom-nameservers/
cluster autoscaler	TBD	https://github.com/kubernetes/autoscaler/tree/master/cluster-autoscaler
kube rbac proxy	TBD	https://github.com/brancz/kube-rbac-proxy
kms plugins	TBD	https://kubernetes.io/docs/tasks/administer-cluster/kms-provider/#implementing-a-kms-plugin
cni plugins	TBD	https://github.com/containernetworking/cni
csi plugins	TBD	https://github.com/kubernetes-csi
aggregator layer	TBD	https://github.com/kubernetes/kube-aggregator

https://github.com/kubernetes/sig-security/blob/main/sig-security-external-audit/external-audit-roadmap.md

Next Audit

https://github.com/kubernetes/sig-security/issues/104

Kubernetes Security Audit
Security Architecture Review

Title	ID	Risk	GitHub k/k Issue	Status
Additive Access Control	NCC-E003660-PA6	Medium	#118982	fix needed
Multiple Concerns with Network Policy	NCC-E003660-XE9	Low	#118983	won't fix
Lack of Cohesion Between Core Access Control Mechanisms	NCC-E003660-DXX	Low	#118985	fix needed
Weakness in Pod Security Standards Restricted Profile	NCC-E003660-UCG	Low	#118987	fix needed

For Reference

Kubernetes Security Audit kube-apiserver

Title	ID	Risk	GitHub k/k Issue	Status
Common Certificate Authority Possible for Client CA and Request Header CA	NCC-E003660-F9W	Medium	#119267	fix needed
Path Traversal in Namespace Specifier	NCC-E003660-RKV	Medium	#119269	fixed
Redirection of API Server Traffic to Kubelet	NCC-E003660-JAV	Medium	#119270	fix needed
API Server Proxy Disables TLS Certificate Validation	NCC-E003660-MRE	Medium	#119625	fix needed
Authentication Source Not Shown in Audit Logs	NCC-E003660-R44	Low	#119626	fix needed
EmptyDir Volumes Do Not Support Mount Options	NCC-E003660-7HM	Low	#119627	fix needed
Loopback Token Usable Externally	NCC-E003660-47W	Low	#119628	fix needed

For Reference

Kubernetes Security Audit kube-apiserver

Title	ID	Risk	GitHub k/k Issue	Status
Inaccurate X-Forwarded-Uri Header	NCC-E003660-HFV	Low	#119629	fix needed
Logging of Incorrect Bootstrap Tokens	NCC-E003660-WVM	Low	#119630	fixed
Incorrect Handling of Proxy Authentication Headers	NCC-E003660-YVU	Low	#119631	fixed
Timing Side Channel in Bootstrap Tokens Generation and Handling	NCC-E003660-TTV	Info	#119632	fixed
Non Constant-Time Comparison of Service Account Token Secrets	NCC-E003660-PCK	Info	#119638	fixed
Low Entropy Bootstrap Tokens	NCC-E003660-WHE	Info	#119639	needs KEP

For Reference

Kubernetes Security Audit kubelet

Title	ID	Risk	GitHub k/k Issue	Status

For Reference

Please scan the QR Code above
to leave feedback on this session