Kubescape

by ARMO

Report date: 2023-06-09T17:26:06

FRAMEWORKS: AllControls (compliance: 63.68), NSA (compliance: 65.59), MITRE (compliance: 71.90)

SEVERITY	CONTROL NAME	FAILED RESOURCES	ALL RESOURCES	% COMPLIANCE-SCORE
Critical	API server insecure port is enabled	0	3	100%
Critical	Disable anonymous access to Kubelet service	0	3	100%
Critical	Enforce Kubelet client TLS authentication	0	3	100%
Critical	CVE-2022-39328-grafana-auth-bypass	0	0	100%
High	Forbidden Container Registries	0	44	Action Required *
High	Resources memory limit and request	0	44	Action Required *
High	Resource limits	26	44	41%
High	Applications credentials in configuration files	0	89	Action Required *
High	List Kubernetes secrets	28	116	76%
High	Host PID/IPC privileges	0	44	100%
High	HostNetwork access	9	44	80%
High	Writable hostPath mount	8	44	82%
High	Insecure capabilities	0	44	100%
High	HostPath mount	6	44	86%
High	Resources CPU limit and request	0	44	Action Required *
High	Instance Metadata API	0	0	100%
High	Privileged container	1	44	98%
High	CVE-2021-25742-nginx-ingress-snippet-annotation-vu...	0	0	100%
High	Workloads with Critical vulnerabilities exposed to...	0	0	Action Required **
High	Workloads with RCE vulnerabilities exposed to exte...	0	0	Action Required **
High	CVE-2022-23648-containerd-fs-escape	0	3	100%
High	RBAC enabled	0	1	100%
High	CVE-2022-47633-kyverno-signature-bypass	0	0	100%
Medium	Exec into container	25	116	78%
Medium	Data Destruction	27	116	77%
Medium	Non-root containers	27	44	39%
Medium	Allow privilege escalation	27	44	39%
Medium	Mount service principal	0	44	100%
Medium	Exposed sensitive interfaces	0	0	100%
Medium	Ingress and Egress blocked	27	45	40%
Medium	Delete Kubernetes events	26	116	78%
Medium	Automatic mapping of service account	54	111	51%
Medium	Cluster-admin binding	16	116	86%
Medium	CoreDNS poisoning	26	116	78%
Medium	Malicious admission controller (mutating)	1	1	0%
Medium	Container hostPort	2	44	95%
Medium	Access container service account	28	66	58%
Medium	Cluster internal networking	6	11	45%
Medium	Linux hardening	27	44	39%
Medium	Configured liveness probe	17	44	61%
Medium	CVE-2021-25741 - Using symlink for arbitrary host ...	0	0	100%
Medium	Sudo in container entrypoint	0	44	100%
Medium	Portforwarding privileges	25	116	78%
Medium	No impersonation	25	116	78%
Medium	Secret/ETCD encryption enabled	1	1	0%
Medium	Audit logs enabled	1	1	0%
Medium	Containers mounting Docker socket	0	44	100%
Medium	Images from allowed registry	0	44	Action Required *
Medium	CVE-2022-0185-linux-kernel-container-escape	3	3	0%
Medium	CVE-2022-24348-argocddirtraversal	0	0	100%
Medium	Workloads with excessive amount of vulnerabilities	0	0	Action Required **
Medium	CVE-2022-0492-cgroups-container-escape	29	44	34%
Low	Access Kubernetes dashboard	0	160	100%
Low	Immutable container filesystem	25	44	43%
Low	Configured readiness probe	21	44	52%
Low	Kubernetes CronJob	0	0	100%
Low	Malicious admission controller (validating)	3	3	0%
Low	SSH server running inside container	0	9	100%
Low	Network mapping	6	11	45%
Low	Pods in default namespace	3	44	93%
Low	PSP enabled	0	1	100%
Low	Naked PODs	0	56	100%
Low	Image pull policy on latest tag	0	44	100%
Low	Label usage for resources	22	44	50%

Low	K8s common labels usage	21	44	52%
	Resource summary	**112**	**344**	**63.90%**

*** failed to pull image scanning data: credentials are not configured for any registry adaptor. for more information: https://hub.armosec.io/docs/configuration-of-image-vulnerabilities**

**** Control configurations are empty**