

Release 5 Security Scan Manual Logs

	Project Name	Scan Tool (vuls, lynis, kube-hunter)	Log Data
1	KNI Industrial Edge	kube-hunter pod. log	<pre>/ # kube-hunter --remote 10.0.0.3 --pod 2021-08-11 09:15:54,691 INFO kube_hunter.modules.report.collector Started hunting 2021-08-11 09:15:54,691 INFO kube_hunter.modules.report.collector Discovering Open Kubernetes Services 2021-08-11 09:15:54,697 INFO kube_hunter.modules.report.collector Found vulnerability "CAP_NET_RAW Enabled" in Local to Pod (85813518b3cf) 2021-08-11 09:15:54,725 INFO kube_hunter.modules.report.collector Found open service "Etcd" at 10.0.0.3:2379 2021-08-11 09:15:54,751 INFO kube_hunter.modules.report.collector Found open service "Kubelet API" at 10.0.0.3:10250 2021-08-11 09:15:54,797 INFO kube_hunter.modules.report.collector Found open service "Unrecognized K8s API" at 10.0.0.3:6443 Nodes +-----+ TYPE LOCATION +-----+ Node/Master 10.0.0.3 +-----+ Detected Services +-----+ SERVICE LOCATION DESCRIPTION +-----+ Unrecognized K8s API 10.0.0.3:6443 A Kubernetes API service +-----+ Kubelet API 10.0.0.3:10250 The Kubelet is the main component in every Node, all pod operations goes through the kubelet +-----+ Etcd 10.0.0.3:2379 Etcd is a DB that stores cluster's data, it contains configuration and current state information, and might contain secrets +-----+ Vulnerabilities For further information about a vulnerability, search its ID in: https://github.com/aquasecurity/kube-hunter/tree/master/docs/_kb +-----+ ID LOCATION CATEGORY VULNERABILITY DESCRIPTION EVIDENCE +-----+ None Local to Pod Access Risk CAP_NET_RAW Enabled CAP_NET_RAW is (85813518b3cf) enabled by default for pods. If an attacker manages to compromise a pod, they could potentially take advantage of this capability to perform network attacks on other pods running on the same node +-----+</pre>

2	KNI Industrial Edge	kube-hunter cluster.log	<pre>/ # kube-hunter --remote 10.0.0.3 2021-08-11 09:16:02,362 INFO kube_hunter.modules.report.collector Started hunting 2021-08-11 09:16:02,363 INFO kube_hunter.modules.report.collector Discovering Open Kubernetes Services 2021-08-11 09:16:02,394 INFO kube_hunter.modules.report.collector Found open service "Etcd" at 10.0.0.3:2379 2021-08-11 09:16:02,433 INFO kube_hunter.modules.report.collector Found open service "Kubelet API" at 10.0.0.3:10250 2021-08-11 09:16:02,468 INFO kube_hunter.modules.report.collector Found open service "Unrecognized K8s API" at 10.0.0.3:6443 Nodes +-----+-----+ TYPE LOCATION +-----+-----+ Node/Master 10.0.0.3 +-----+-----+ Detected Services +-----+-----+-----+ SERVICE LOCATION DESCRIPTION +-----+-----+-----+ Unrecognized K8s API 10.0.0.3:6443 A Kubernetes API service +-----+-----+-----+ Kubelet API 10.0.0.3:10250 The Kubelet is the main component in every Node, all pod operations goes through the kubelet +-----+-----+-----+ Etcd 10.0.0.3:2379 Etcd is a DB that stores cluster's data, it contains configuration and current state information, and might contain secrets +-----+-----+-----+ No vulnerabilities were found</pre>
---	-------------------------------------	-------------------------	---

3	KNI Provider Access Edge	kube-hunter pod. log	<pre> / # kube-hunter --remote 10.0.0.3 --pod 2021-08-11 09:15:54,691 INFO kube_hunter.modules.report.collector Started hunting 2021-08-11 09:15:54,691 INFO kube_hunter.modules.report.collector Discovering Open Kubernetes Services 2021-08-11 09:15:54,697 INFO kube_hunter.modules.report.collector Found vulnerability "CAP_NET_RAW Enabled" in Local to Pod (85813518b3cf) 2021-08-11 09:15:54,725 INFO kube_hunter.modules.report.collector Found open service "Etcd" at 10.0.0.3:2379 2021-08-11 09:15:54,751 INFO kube_hunter.modules.report.collector Found open service "Kubelet API" at 10.0.0.3:10250 2021-08-11 09:15:54,797 INFO kube_hunter.modules.report.collector Found open service "Unrecognized K8s API" at 10.0.0.3:6443 Nodes +-----+ TYPE LOCATION +-----+ Node/Master 10.0.0.3 +-----+ Detected Services +-----+ SERVICE LOCATION DESCRIPTION +-----+ Unrecognized K8s API 10.0.0.3:6443 A Kubernetes API service +-----+ Kubelet API 10.0.0.3:10250 The Kubelet is the main component in every Node, all pod operations goes through the kubelet +-----+ Etcd 10.0.0.3:2379 Etcd is a DB that stores cluster's data, it contains configuration and current state information, and might contain secrets +-----+ Vulnerabilities For further information about a vulnerability, search its ID in: https://github.com/aquasecurity/kube-hunter/tree/master/docs/_kb +-----+ ID LOCATION CATEGORY VULNERABILITY DESCRIPTION EVIDENCE +-----+ None Local to Pod Access Risk CAP_NET_RAW Enabled CAP_NET_RAW is (85813518b3cf) enabled by default for pods. If an attacker manages to compromise a pod, they could potentially take advantage of this capability to perform network attacks on other pods running on the same node +-----+ </pre>
---	--	-------------------------	--

4	KNI Provider Access Edge	kube-hunter cluster.log	<pre> / # kube-hunter --remote 10.0.0.3 2021-08-11 09:16:02,362 INFO kube_hunter.modules.report.collector Started hunting 2021-08-11 09:16:02,363 INFO kube_hunter.modules.report.collector Discovering Open Kubernetes Services 2021-08-11 09:16:02,394 INFO kube_hunter.modules.report.collector Found open service "Etcd" at 10.0.0.3:2379 2021-08-11 09:16:02,433 INFO kube_hunter.modules.report.collector Found open service "Kubelet API" at 10.0.0.3:10250 2021-08-11 09:16:02,468 INFO kube_hunter.modules.report.collector Found open service "Unrecognized K8s API" at 10.0.0.3:6443 Nodes +-----+-----+ TYPE LOCATION +-----+-----+ Node/Master 10.0.0.3 +-----+-----+ Detected Services +-----+-----+-----+ SERVICE LOCATION DESCRIPTION +-----+-----+-----+ Unrecognized K8s API 10.0.0.3:6443 A Kubernetes API service +-----+-----+-----+ Kubelet API 10.0.0.3:10250 The Kubelet is the main component in every Node, all pod operations goes through the kubelet +-----+-----+-----+ Etcd 10.0.0.3:2379 Etcd is a DB that stores cluster's data, it contains configuration and current state information, and might contain secrets +-----+-----+-----+ No vulnerabilities were found </pre>
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			

27			
28			
29			
30			
31			
32			