EKS Protection finding types

PDF | RSS

The following findings are specific to Amazon EKS resources and have a resource type of

and details of the findings differ based on finding type.

For all EKS audit logs type findings we recommend that you examine the resource in question to determine if the activity is expected or potentially malicious

ing a compromised EKS audit logs resource identified by a GuardDuty finding, see Remediating EKS Protection findings.

Note

If

use of which this finding

x p e c t e d , c o n s i d e r a d d i n g

inGuardDutytoprevent future alerts.

alAccess:Kubernetes/MaliciousIPCaller

- CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

alAccess:Kubernetes/TorIPCaller

- DefenseEvasion:Kubernetes/MaliciousIPCaller
- DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

uber
nete
s/Su
cces
sful
Ano
nym
ous
Acce
ss

- Defe
nseE
vasi
on:K
uber
nete
s/To
rIPC
aller
- Disc
over
y:Ku
bern
etes

.Custom

- Discovery:Kubernetes/SuccessfulAnonymousAccess
- Discovery:Kubernetes/TorIPCaller
- Execution:Kubernetes/ExecInKubeSystemPod

tes/Maliciou sIPCaller

- Impact: Kubernetes/MaliciousIPCaller.Custom
- Impact: Kubernetes/

istence:Kubernetes/ContainerWithSensitiveMount

- Persistence:Kubernetes/MaliciouslPCaller

ce:K
uber
nete
s/Su
cces
sful
Ano
nym
ous
Acce
ss

- Pers
isten
ce:K
uber
nete
s/To
rIPC
aller
- Poli
cy:K
uber
nete
s/Ad
mini
Acce
ssTo
Defa
ultS
ervic
eAcc
ount

s/Anonymous AccessGranted

- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/KubeflowDashboardExposed
- PrivilegeEscalation:Kubern

onta
iner

- Cred
enti
alAc
cess:
Kub
erne
tes/
Ano
mal
ous
Beh
avio
r.Sec
rets
Acce
ssed
- Privi
lege
Esca
latio
n:Ku
bern
etes/
Anom
alous
Beh
avio
r.Rol
eBin
ding

n:Kubernetes/AnomalousBehavior.ExecInPod

- Privilege Escalation:Kubernetes/AnomalousBehavior.WorkloadDeployedPrivilegedContainer

netes/Anomalous Behavior.WorkloadDeployed!ContainerWithSensitiveMount

- Execution:Kubernetes/Anomalous Behavior.WorkloadDeployed

n:Kubernetes/AnomalousBehavior.RoleCreated

- Discovery:Kubernetes/AnomalousBehavior.Per
missionC

Note

B
e
f
o
r

e r n e t e s v e r s i o n 1 . 1 4 , t h e

```
t
i
c
a
t
e
d
g
r
o
u
p
w
a
s
a
s
s
o
c
i
```

```
    cover yand system:basic
```

s by default. This associati

t
e
n
d
e
d
a
c
c
e
s
s
f
r
o
m
a
n
o
n
y
m

updates on revoked subscriptions

CredentialAccess:Kubernetes/MaliciousIPCaller

CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

CredentialAccess:Kubernetes/SuccessfulAnonymousAccess

CredentialAccess:Kubernetes/TorIPCaller

DefenseEvasion:Kubernetes/MaliciousIPCaller

DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess

DefenseEvasion:Kubernetes/TorIPCaller

Discovery:Kubernetes/MaliciousIPCaller

Discovery:Kubernetes/MaliciousIPCaller.Custom

Discovery:Kubernetes/SuccessfulAnonymousAccess

Discovery:Kubernetes/TorIPCaller

Execution:Kubernetes/ExecInKubeSystemPod

Impact:Kubernetes/MaliciousIPCaller

Impact:Kubernetes/MaliciousIPCaller.Custom

Impact:Kubernetes/SuccessfulAnonymousAccess

n i f y o u u p d a t e d y o u r c l u s t

r h i g h e r , t h e s e p e r m i s s i o

led. We recommend that you

e p e r m i s s i o n s f r o m t h e s y s t e m : s e r v i c e a c c o u n t : k u b e - s y s t e m : d e f a u l t t h e

```
        attedgroup.Forguidanceon
```

ermissions, see Security best practice

Amazon EKS in the *Amazon EKS User Guide*.

lAccess:Kubernetes/MaliciousIPCaller

An API commonly used to access credentials or secrets in a Kubernetes cluster was invoked from a

addre ss.

Default severity : High

- **Feature:** EKS audit logs

This finding informs you that an API operation was invoked from an IP address that is associated with known malicious activity. The API observe

d with the credential access tactics where an adversary is attempting to collect passwords, usernames, and access keys for your Kubernetes cluster.

Remediation recommendations:

If the user reported in the finding under

`s` section is `system:anonymous`, investigate why the anonymous user was permitted to invoke the API and revoke the permissions, if needed. by following the recommendations in Security best practices for Amazon EKS in

	the user is an authenticated user, investigate to determine if the activity was legitimate or malicious. If the activity was malicious revoke access of the user and reverse any changes an adversary to your cluster. For more information, see Remedia

CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

An API commonly used to access credentials or secrets in a Kubernetes

from an IP address on a custom threat list.

Default severity: High

- **Feature:** EKS audit logs

This finding informs you that an API operation was invoked from an IP address that is

you uploaded. The threat list associated with this finding is listed in the **Additional Information** section of a finding's details. The API observed is

usernames, and access keys for your Kubernetes cluster.

Remediation recommendations:

If the user reported in the finding under the `KubernetesUserDetails` section is `system:anonymous`, investigate why the

d to invoke the API and and revoke the permissions, if needed, by following the instructions in Security best practices for Amazon EKS in the *Amazon EKS User Guide*. If the IAM authenticated user, investigate to determine if the activity

s. If the activity was malicious revoke access of the user and reverse any changes made by an adversary to your cluster. For more information, see Remediating EKS Protection findings.

Credential Access:Kubernetes/

nymousAccess

An API commonly used to access credentials or secrets in a Kubernetes cluster was invoked by an unauthenticated user.

Default severity

EKS audit logs

This finding informs you that an API operation was successfully invoked by the `system:anonymous` user. API calls made by `system:anonymous` are unauthenticated. The observed API is commonly associated with

where an adversary is attempting to collect passwords, usernames, and access keys for your Kubernetes cluster. This activity indicates that anonymous or unauthenticated [illegible] d on the API action reported in the finding and may be

If this behavior is not expected, it may indicate a configuration mistake or that your credentials are compromised.

Remediation recommendations:

You should

permissions that have been granted to the system

and ensure that all the permissions are needed. If the permissions were granted mistakenly or maliciously, you should revoke access of the user and reverse any changes made by

y to your cluster. For more information, see Security best practices

Amazon EKS User Guide.

For more information, see Remediating EKS Protection findings.

CredentialAccess:Kubernetes/TorIPCaller

An API commonly used to

secrets in a Kubernetes cluster was invoked from a Tor exit node IP address.

Default severity: High

- **Feature:** EKS audit logs

This finding informs you that an API

node IP address. The API observed is commonly associated with the credential access tactics where an adversary is attempting to collect passwords, usernames, and access keys for Kubernetes cluster. Tor is software for enabling anonym

encrypts and randomly bounces communications through relays between a series of network nodes. The last Tor node is called the exit node. This can indicate unauthorized access to Kubernetes cluster resources with the intent of hiding the

Remediation recommendations:

If the user reported in the finding under the `KubernetesUserDetails` section is `system:anonymous`, investigate why the anonymous user was permitted to invoke the API and revoke

by following the instructions in Security best practices for Amazon EKS in the *Amazon EKS User Guide*. If the user is an authenticated user, investigate to determine if the activity legitimate or malicious. If the activity was malicious revoke

any changes made by an adversary to your cluster. For more information, see Remediating EKS Protection findings.

DefenseEvasion:Kubernetes/AnomalousPCaller

An API

evade defensive measures was invoked from a known malicious IP address.

Default severity: High

- Feature: EKS audit logs

This finding informs you that

	from an IP address that is associated with known malicious activity. The API observed is commonly associated with defense evasion tactics where an adversary is trying to hide actions to avoid detection. Remediation recomm

user reported in the finding under the `KubernetesUserDetails` section is `system:anonymous`, investigate why the anonymous user was permitted to invoke the API revoke the permissions, if needed, by following the

practices for Amazon EKS in the *Amazon EKS User Guide*. If the user is an authenticated user, investigate to determine if the activity was legitimate or malicious. If the activity was malicious, revoke access of the user and reverse any changes made by

For more information, see Remediating EKS Protection findings.

DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

An API commonly used to evade

was invoked from an IP address on a custom threat list.

Default severity: High

- **Feature:** EKS audit logs

finding informs you that an API operation was invoked from an

on a threat list that you uploaded. The threat list associated with this finding is listed in the **Additional Information** section of a finding's details.

The API observed is typically associated with defense evasion tactics where an adversar

actions to avoid detection.

Remediation recommendations:

If the user reported in the finding under the `KubernetesUserDetails` section is system:serviceaccount:anonymous, investigate why the anonymous user was permitte

revoke the permissions, if needed, by following the instructions in Security best practices for Amazon EKS in the *Amazon EKS User Guide*. If the user is an authenticated

te to determine if the activity was legitimate or maliciou

s revoke access of the user and reverse any changes made by an adversary to your cluster. For more information, see Remediating EKS Protection findings.

An API commonly used to evade defensive measures was invoked by an unauthenticated user.

Default

- Feature: EKS audit logs

an API operation was successfully invoked by the `system:anonymous` user. API calls made by `system:anonymous` are unauthenticated. The observed API is commonly associate

evasion tactics where an adversary is trying to hide

	n. This activity indicates that anonymous or unauthenticated access is permitted on the API action reported in the finding and may be permitted on other actions. if this behavior is not , it may indicate a configuration mistake or that your

Remediation recommendations:

You should examine the permissions that have been granted to the `system:anonymous` user on your cluster and ensure that all permissions are needed. If the permissions were granted by mistaken

revoke access of the user and reverse any changes made by an adversary to your cluster. For more information, see Security best practices for Amazon EKS in the *Amazon EKS User Guide*. For more information, see Remediating EKS Protection findings.

vasion:Kubernetes/TorIPCaller	An API commonly used to evade defensive measures was invoked from a Tor exit node IP address.

- **Feature:** EKS audit logs

  This finding informs you that an API was invoked from a Tor exit node IP address. The API observed is commonly associated with evasion tactics where an adversary is trying to hide their

software for enabling anonymous communication. It encrypts and randomly bounces communications through relays between a series of network nodes. The last Tor node

node. This can indicate unauthorized access to your Kuberne

hiding the adversary's true identity.

Remediation recommendations:

If the user reported in the finding under the `KubernetesUserDetails` section is anonymous, investigate why the anonymous user was

and revoke the permissions, if needed, by following the instructions in Security best practices for Amazon EKS in the *Amazon EKS User Guide*. If the user is an authenticated investigate to determine if the activity was legitimate or

	malicious revoke access of the user and reverse any changes made by an adversary to your cluster. For more information, see Remediating EKS Protection findings.

An API commonly used to discover resources in a Kubernetes cluster was invoked from an IP address.

Default severity: Medium

- Feature: EKS audi

finding informs you that an API operation was invoked from an IP address that is associated with known malicious activity. The observed API is commonly used with the discovery stage of an attack wherein an attacker is gathering information

tes cluster is susceptible to a broader attack.

For unauthenticated access

M a l i c i o u s I P C a l l e r f i n d i n

enotgeneratedforunauth

Successful Anonymous Access

e
n
e
r
a
t
e
d
f
o
r
u
n
a
u
t
h
e
n
t
i
c

c
c
e
s
s
.

Remediation recommendations:

If the user reported in the finding under the `KubernetesUserDetails` `system:anonymous`, investigate why the anonym

invoke the API and revoke the permissions, if needed, by following the instructions in Security best practices for Amazon EKS in the *Amazon EKS User Guide*. If the user is a compromised user, investigate to determine if the activity was

activity was malicious revoke access of the user and reverse any changes made by an adversary to your cluster. For more information, see Remediating EKS Protection findings.

stom

An API commonly used to discover resources in a Kubernetes cluster was invoked from an IP address on a custom threat list.

- **Feature:** EKS audit logs

This finding informs you that an API was invoked from an IP address that is included on a threat list that you uploade

section of a finding's details. The observed API is commonly used with the discovery stage of an attack wherein an attacker is gathering information to determine if your Kubernetes cluster is susceptible to a broader attack.

Remediation

If the user reported in the finding under the `KubernetesUserDetails` section is `system:anonymous`, investigate why the anonymous user was permitted to invoke and revoke the permissions, if needed, by following

best practices for Amazon EKS in the *Amazon EKS User Guide*. If the user is an authenticated user, investigate to determine if the activity was legitimate or malicious. If the activity was malicious revoke access of the user and reverse any changes

cluster. For more information, see Remediating EKS Protection findings.

Discovery:Kubernetes/SuccessfulAnonymousAccess

An API commonly used to

in a Kubernetes cluster was invoked by an unauthenticated user.

Default severity: Medium

- **Feature:** EKS audit
This finding informs you that an API operation was successf

`:anonymous` user. API calls made by `system:anonymous` are unauthenticated. The observed API is commonly associated with the discovery stage of an attack when an adversary is gathering information on your Kubernetes cluster.

	anonymous or unauthenticated access is permitted on the API action reported in the finding and may be permitted on other actions. If this behavior is not expected, it may indicate misconfiguration mistakes or that your credentials are compromised.

the health check API endpoints such as `/healthz`, `/livez`, `/readyz`, and `/version`.

Remediation recommendations:

You should examine the permissions that have been granted to the `system:anonymous` user on your

the permissions are needed. If the permissions were granted mistakenly or maliciously, you should revoke access of the user and reverse any changes made by an adversary to your cluster. For more information, see Security best practices for Amazon EKS in

For more information, see Remediating EKS Protection findings.

Discovery:Kubernetes/TorIPCaller

An API [illegible] only used to discover resources

r was invoked from a Tor exit node IP address.

Default severity: Medium

- **Feature:** EKS audit logs

This finding informs you that an API was invoked from a Tor exit node IP

commonly used with the discovery stage of an attack wherein an attacker is gathering information to determine if your Kubernetes cluster is susceptible to a broader attack. Tactic for enabling anonymous communication, it encrypts

	communications through relays between a series of network nodes. The last Tor node is called the exit node. This can indicate unauthorized access to your Kubernetes cluster with the intent of hiding the adversary's true identity.
	Remediation recomm

user reported in the finding under the `KubernetesUserDetails` section is `system:anonymous`, investigate why the anonymous user was permitted to invoke the API. Revoke the permissions, if needed, by following the

practices for Amazon EKS in the *Amazon EKS User Guide*. If the user is an authenticated user, investigate to determine if the activity was legitimate or malicious. If the activity was malicious, revoke access of the user and reverse any changes made by

For more information, see Remediating EKS Protection findings.

Execution:Kubernetes/ExecInKubeSystemPod

m name space

Default severity: Medium

- **Feature:** EKS audit logs

This finding informs you that a command was executed in a pod with the kube-system namespace using Kubernetes exec

ce is a default namespaces, which is primarily used for system level components such as `kube-dns` and `kube-proxy`. It is very uncommon to execute commands inside pods or containe

system namespace and may indicate suspicio

ation recommendations:	If the execution of this command is unexpected, the credentials of the user identity used to execute the command may be compromised. Revoke access of and reverse any changes made by an adversary to your

Remediating EKS Protection findings.

Impact:Kubernetes/MaliciousIPCaller

An API commonly used to tamper with resources in a Kuber

invoked from a known malicious IP address.

Default severity: High

- **Feature:** EKS audit logs

This finding informs you that an API operation was invoked from an IP address that is

s activity. The observed API is commonly associated with impact tactics where an adversary is trying to manipulate, interrupt, or destroy data within your AWS environment.

Remediation recommendations:

finding under the `KubernetesUserDetails` section is `system:anonymous`, investigate why the anonymous user was permitted to invoke the API and revoke permissions, if needed, by following the instructions in

Amazon EKS in the *Amazon EKS User Guide*. If the user is an authenticated user, investigate to determine if the activity was legitimate or malicious. If the activity was malicious, revoke the user and reverse any changes made by an adversar

ion, see Remediating EKS Protection findings.

Impact:Kubernetes/MaliciousIPCaller.Custom

An API comm… used to tamper with resources

r was invoked from an IP address on a custom threat list.

Default severity: High

- **Feature:** EKS audit logs

finding informs you that an API operation was invoked from an

on a threat list that you uploaded. The threat list associated with this finding is listed in the **Additional Information** section of a finding's details.

The observed API is typically associated with impact tactics where an adversary is

, or destroy data within your AWS environment.

Remediation recommendations:

If the user reported in the finding under the `KubernetesUserDetails` section is `system:anonymous`, investigate why the

d to invoke the API and revoke the permissions, if needed, by following the instructions in Security best practices for Amazon EKS in the *Amazon EKS User Guide*. If the user is authenticated user, investigate to determine if the activity

s. If the activity was malicious revoke access of the user and reverse any changes made by an adversary to your cluster. For more information, see Remediating EKS Protection findings.

Impact:Kubernetes/SuccessfulAnonymousAccess

ccess

An API commonly used to tamper with resources in a Kubernetes cluster was invoked by an unauthenticated user.

Default severity: High

t logs

This finding informs you that an API operation was successfully invoked by the `system:anonymous` user. API calls made by `system:anonymous` are unauthenticated. The observed API is commonly associated with the impact

y is tamperin g with resource s in your cluster. This activity indicates that anonym ous or unauthe nticated access is permitte d on the API action reported in the finding and may be

other actions. If this behavior is not expected , it may indicate

or that your credentials are compromised.

Remediation recommendations:

You should examine the permissions that have been granted to the system:anonym on your cluster and ensure that all the permissions are

granted mistakenly or maliciously, you should revoke access of the user and reverse any changes made by an adversary to your cluster. For more information, see Security best practices for EKS in the *Amazon EKS User Guide*.

For more informat

on findings.

Impact:Kubernetes/TorIPCaller

An API commonly used to tamper with resources in a Kubernetes cluster was invok

node IP address.

Default severity: High

- **Feature:** EKS audit logs

This finding informs you that an API was invoked from a Tor exit address. The API observed is commonly associated with

y is trying to manipulate, interrupt, or destroy data within your AWS environment.

Tor is software for enabling anonymous communication. It encrypts and randomly bounces communications through relays between a series of

is called the exit node. This can indicate unauthorized access to your Kubernetes cluster with the intent of hiding the adversary's true identity.

Remediation recommendations:

is `system:anonymous`, investigate why the anonymous user was permitted to invoke the API and revoke the permissions, if needed, by following the instructi

best practices for Amazon EKS in the *Amazon*

	authenticated user, investigate to determine if the activity was legitimate or malicious. If the activity was malicious revoke access of the user and reverse any changes made by it.
	y to your cluster. For more information, see Remediating EKS Protecti

Persistence:Kubernetes/ContainerWithSensitiveMount

A container was launched with a sensitive external host path mounted

severity: Medium

- **Feature:** EKS audit logs

This finding informs you that a container was launched with a configuration that included a path with write access in the volumeMounts

sensitive host path accessible and writable from inside the container. This technique is commonly used by adversaries to gain access to the host's filesystem.

Remediation recommendations:

If this container launch

	als of the user identity used to launch the container may be compromised. Revoke access of the user and reverse any changes made by an adversary to your cluster. For more information about investigating EKS Protection findings. If this container launch

ended that you use a suppression rule consisting of a filter criteria based on the `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` field. In the filter the `imagePrefix` field should be same as the `imageP`

To learn more about creating suppression rules see Suppression rules.

Persistence:Kubernetes/MaliciousIPCaller

API commonly used to obtai

to a Kubernetes cluster was invoked from a known malicious IP address.

Default severity: Medium

- Feature: EKS Audit Logs

This finding informs you that

from an IP address that is associated with known malicious activity. The API observed is commonly associated with persistence tactics where an adversary has gained access to [illegible] cluster and is attempting to maintain that access.

ns:

If the user reported in the finding under the `KubernetesUserDetails` section is `system:anonymous`, investigate why the anonym

ons in Security best practices for Amazon EKS in the *Amazon EKS User Guide*. If the user is an authenticated user, investigate to determine if the activity was legitimate or malicious revoke access of the user and reverse

adversary to your cluster. For more information, see Remediating EKS Protection findings.

Persistence:Kubernetes/MaliciousIPCaller.Custom

An API commonly used

persistent access to a Kubernetes cluster was invoked from an IP address on a custom threat list.

Default severity:

- Feature: EKS audit logs

an API operation was invoked from an IP address that is included on a threat list that you uploaded. The threat list associated with this finding is listed in the Additional information section of a finding's details. The API observed is

persistence tactics where an adversary has gained access to your Kubernetes cluster and is attempting to maintain that access.

Remediation recommendations:

If the

in the finding under the `KubernetesUserDetail`

`:anonymous`, investigate why the anonymous user was permitted to invoke the API and revoke the permissions, if needed, by following the instructions in Security for Amazon EKS in the *Amazon EKS User Guide*. If the user

	investigate to determine if the activity was legitimate or malicious. If the activity was malicious revoke access of the user and reverse any changes made by an adversary to your cluster. For information, see Remediating EKS Protection findings.

e:Kubernetes/SuccessfulAnonymousAccess

An API commonly used to obtain high-level

to a Kubernetes cluster was invok

ated user.

Default severity: High

- **Feature:** EKS audit logs

This finding informs you that an API operation was successfully invoked by the system:anonymous user. API calls made by system:anonymous are

d API is commonly associated with the persistence tactics where an adversary has gained access to your cluster and is attempting to maintain that access. This activity indicates that

ous or unauthenticated access is permitted on the API action

be permitted on other actions. If this behavior is not expected, it may indicate a configuration mistake or that your credentials are compromised.

Remediation recommendations:

You should examine the permissions that

`system:anonymous` user on your cluster and ensure that all the permissions are needed. If the permissions were granted mistakenly or maliciously, you should revoke access of the user and any changes made by an adversary to your cluster. For more

practices for Amazon EKS in the *Amazon EKS User Guide*.

For more information, see Remediating EKS Protection findings.

Persistence:Kubernetes/ContainerWithSensitiveMount

n persistent access to a Kubernetes cluster was invoked from a Tor exit node IP address.

Default severity:

- Feature: EKS audit logs

	an API was invoked from a Tor exit node IP address. The API observed is commonly associated with persistence tactics where an adversary has gained access to your Kubernetes cluster attempting to maintain that access. Tor is software for

ication. It encrypts and randomly bounces communications through relays between a series of network nodes. The last Tor node is called the exit node. This can indicate unauthorized your AWS resources with the intent of hiding the

Remediation recommendations:

If the user reported in the finding under the `KubernetesUserDetails` section is `system:anonymous`, investigate why the anonymous user was permitted to invoke the API and revoke

by following the instructions in Security best practices for Amazon EKS in the *Amazon EKS User Guide*. If the user is an authenticated user, investigate to determine if the activity legitimate or malicious. If the activity was malicious revoke

any changes made by an adversary to your cluster. For more information, see Remediating EKS Protection findings.

Policy:Kubernetes/AdmittedToDefaultServiceAc

The default service account was granted admin privileges on a Kubernetes cluster.

Default severity: High

EKS audit logs

This finding informs

account for a namespace in your Kubernetes cluster was granted admin privileges. Kubernetes creates a default service account for all the namespaces in the cluster automatically assigns the default service account as an

	been explicitly associated to another service account. If the default service account has admin privileges, it may result in pods being unintentionally launched with admin privileges. If this is not expected, it may indicate a configuration mistake

compromised.

Remediation recommendations:

You should not use the default service account to grant permissions to pods. Instead you should create a dedicated service account for each workload and grant permission to that

fix this issue, you should create dedicated service accounts for all your pods and workloads and update the pods and workloads to migrate from the default service account to their dedicated accounts. Then you should remove the admin permissi

account. For more information, see Remediating EKS Protection findings.

Policy:Kubernetes/AnonymousAccessGranted

The system:anonymous user was grant

on a Kubernetes cluster.

Default severity: High

- **Feature:** EKS audit logs

This finding informs you that a user on your Kuberne successfully created a ClusterRoleBinding or

	`system:anonymous` to a role. This enables unauthenticated access to the API operations permitted by the role. If this behavior is not expected, it may indicate a configuration
	your credentials are compromised
	Remediation

You should examine the permissions that have been granted to the `system:anonymous` user or `system:unauthenticated` group on your cluster and revoke unnecessary anonymous access. For more information, see Security best practices

Amazon EKS User Guide. If the permissions were granted maliciously, you should revoke access of the user that granted the permissions and reverse any changes made by an adversar

For more information, see Remediating EKS Protection findings.

bernetes/ExposedDashboard

The dashboard for a Kubernetes cluster was exposed to the internet

finding informs you that Kubernetes dashboard for your cluster was exposed to the internet by a Load Balancer service. An exposed dashboard makes the management interface of your cluster accessible from the internet and allows adversari

cation and access control gaps that may be present.

Remediation recommendations:

You should ensure that strong authentication and authorization is set for Kubernetes Dashboard. You should also impleme

to restrict access to the dashboard from specific IP addresses.

For more information, see Remediating EKS Protection findings.

Policy:Kubernetes/KubeflowDashboardExposed

oard for a Kubernetes cluster was exposed to the Internet

Default severity: Medium

- **Feature:** EKS audit logs

finding informs you that Kubeflow dashboard for your

Internet by a Load Balancer service. An exposed **Kubeflow** dashboard makes the management interface of your **Kubeflow** environment accessible from the Internet and adversaries to exploit any authentication and access

present.

Remediation recommendations:

You should ensure that strong authentication and authorization is enforced on **Kubeflow** Dashboard. You should implement network access control to restrict access to

IP addresses.

For more information, see Remediating EKS Protection findings.

Privilege Escalation:Kubernetes/PrivilegedContainer

A privil

with root level access was launched on your Kubernetes cluster.

Default severity: Medium

- **Feature:** EKS audit
- This finding informs you that a privileged containe

tes cluster using an image has never before been used to launch privileged containers in your cluster. A privileged container has root level access to the host ies can launch privileged containers as a privilege escalatio

compromise the host.

Remediation recommendations:

If this container launch is unexpected, the credentials of the user identity used to launch the container may be

Revoke access of the user and reverse any changes

cluster. For more information, see Remediating EKS Protection findings.

CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed

A Kuber

used to access secrets was invoked in an anomalous way.

Default severity: Medium

- **Feature:** EKS audit logs

finding informs you that an anomalous API operation to

was invoked by a Kubernetes user in your cluster. The observed API is commonly associated with credential access tactics that can lead to privileged escalation and further

your cluster. If this behavior is not expected, it may indicate

	or that your AWS credentials are compromised.
	The observed API was identified as anomalous by the GuardDuty anomaly detection machine learning (ML) model. The ML model evaluates all user API activity within your EKS cluster

	us events that are associated with techniques used by unauthorized users. The ML model tracks multiple factors of the API operation such as the user making the request, the request was made from, user agent used,

operated. You can find the details of the API request that are unusual, in the finding details panel in the GuardDuty console.

Remediation recommendations:

Examine permissions granted to the Kubernetes user in your cluster

permissions are needed. If the permissions were granted mistakenly or maliciously, revoke user access and reverse any changes made by an unauthorized user to your

information, see Remediating EKS Protection findings.

compromised, see Remediating potentially compromised AWS credentials.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCr

A RoleBinding or ClusterRoleBinding to an overly permissive role or sensitive namespace was created or modified in your Kubernetes cluster.

*

Note

This finding's default severity is

um. However, if a RoleBind

Binding involves the Clus

```
    lusterr-admin,theseverity:High
```

t logs

This finding informs you that a user in your Kubernetes cluster created a `RoleBinding` or `ClusterRoleBinding` to bind a user to a role with admin permissions or access to namespaces. If this behavior is not expected, it may indicate

	or that your AWS credentials are compromised.
	The observed API was identified as anomalous by the GuardDuty anomaly detection machine learning (ML) model. The ML model evaluates all user API activity within your EKS cluster.

s anomalous events that are associated with the techniques used by an unauthorized user. The ML model also tracks multiple factors of the API operation, such as the making the request, the location the request was

used, and the namespace that the user operated. You can find the details of the API request that are unusual, in the finding details panel in the GuardDuty console.

Remediation recommendations:

Examine the permissions granted

permissions are defined in the role and subjects involved in `RoleBinding` and `ClusterRoleBinding`. If the permissions were granted mistakenly or maliciously, revoke user reverse any changes made by an unauthorized

information, see Remediating EKS Protection findings.

If your AWS credentials are compromised, see Remediating potentially compromised AWS

Execution:Kubernetes/Ano

or.Exec\nIn Pod

A command was executed inside a pod in an anomalous way.

Default severity: Medium

Feat
EKS audit logs

This finding informs

executed in a pod using the Kubernetes exec API. The Kubernetes exec API allows running arbitrary commands in a pod. If this behavior is not expected for the user, namespace, or cluster, it may indicate either a configuration mistake or that your AWS

	The observed API was identified as anomalous by the GuardDuty anomaly detection machine learning (ML) model. The ML model evaluates all user API activity within your EKS cluster. This ML model also identifies anomalous

the techniques used by an unauthorized user. The ML model also tracks multiple factors of the API operation, such as the user making the request, the location the request was made from, the user agent used, and the namespa

find the details of the API request that are unusual, in the finding details panel in the GuardDuty console.

Remediation recommendations:

If the execution of this unexpected, the credentials of the user identity used to

	have been compromised. Revoke user access and reverse any changes made by an unauthorized user to your cluster. For more information, see Remediating EKS Protection findings. If your AWS credentials are compromised, see

compromised AWS credentials.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadModifiedPrivilegedContainer

launched with a privileged container in an anomalous way.

Default severity: High

- **Feature:** EKS audit logs

This finding informs you that a workload was launched with a privileged

	EKS cluster. A privileged container has root level access to the host. Unauthorized users can launch privileged containers as a privilege escalation tactic to first gain the host and then compromise it. The observed

	modification was identified as anomalous by the GuardDuty anomaly detection machine learning (ML) model. The ML model evaluates all user API and container image activity within your EKS cluster. This ML model also identifies anomalous events

techniques used by an unauthorized user. The ML model also tracks multiple factors of the API operation, such as the user making the request, the location the request made from, the user agent used, container images observe

ce that the user operated. You can find the details of the API request that are unusual, in the finding details panel in the GuardDuty console.

Remediation recommendations:

the container may have been compromised. Revoke user access and reverse any changes made by an unauthorized user to your cluster. For more information, see Protection findings.

If your AWS credentials are

ting potentially compromised AWS credentials.

If this container launch is expected, it is recommended that you use a suppression rule with a filter criteria based on the resource.KubernetesDetails.KubernetesWorkloadDetails.co

the filter criteria, the `imagePrefix` field must have the same value as the `imagePrefix` field specified in the finding. For more information, see Suppression rules in GuardDu

Persistence:Kubernetes/

havior.WorkloadDeployed!Container With Sensitive Mount

A workload was deployed in anomalous way, with a sensitive host

the workload.

Default severity: High

- **Feature:** EKS audit logs

This finding informs you that a workload was launched with a container that included a sensitive host path in the `volumeMounts`

	the sensitive host path accessible and writable from inside the container. This technique is commonly used by unauthorized users to gain access to the host's file
	The observed container creation or

anomalous by the GuardDuty anomaly detection machine learning (ML) model. The ML model evaluates all user API and container image activity within your EKS cluster. This ML model also evaluates anomalous events that are associated with the

rized user. The ML model also tracks multiple factors of the API operation, such as the user making the request, the location the request was made from, the ASN used, container images observed in your account, and the namespa

find the details of the API request that are unusual, in the finding details panel in the GuardDuty console.

Remediation recommendations:

If this

	been compromised. Revoke user access and reverse any changes made by an unauthorized user to your cluster. For more information, see Remediating EKS Protection findings if your AWS credentials are compromised, see Remediating

mised AWS credentials.

If this container launch is expected, it is recommended that you use a suppression rule with a filter criteria based on the resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix field. In

refix field must have the same value as the imageP refix field specified in the finding. For more information, see Suppression rules in GuardDuty.

Exec
n:Ku
bern
etes/
Ano
malo
usBe

adDeployed

A workload was launched in an anomalous way.

Default severity: Low*

Note

ity is Low. However, if the

a p o t e n t i a l l y s u s p i c i o u s

a k n o w n p e n t e s t t o o l , o r a c

potentially suspicious c

u
c
h
a
s
r
e
v
e
r
s
e
s
h
e
l
l
c
o
m
m
a
n
d
t
h
e
n
t
h
e
s

i t y o f t h i s f i n d i n g t y p e w i

Medium.

- **Feature:** EKS audit logs

This finding informs you that a Kubernetes workload was created or modified in an anomalous way, such as an API activity, new

d configuration, within your Amazon EKS cluster. Unauthorized users can launch containers as a tactic to execute arbitrary code to first gain access to the host and then compromise it. The observed container creation or modifica

us by the GuardDuty anomaly detection machine learning (ML) model. The ML model evaluates all user API and container image activity within your EKS cluster. This ML model also identifies anomalous events that are associated with the techniqu

user. The ML model also tracks multiple factors of the API operation, such as the user making the request, the location the request was made from, the user agent, container images observed in your account, and the namespace that

details of the API request that are unusual, in the finding details panel in the GuardDuty console.

Remediation recommendations:

If this container launch is

compromised. Revoke user access and reverse any changes made by an unauthorized user to your cluster. For more information, see Remediating EKS Protection findings.

If your AWS credentials are compromised, see Remediating

AWS credentials.

If this container launch is expected, it is recommended that you use a suppression rule with a filter criteria based on the `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.imagePrefix` field. In the filter

field must have the same value as the `imagePrefix` field specified in the finding. For more information, see Suppression rules in GuardDuty.

.Role Created

A highly permissive Role or ClusterRole was created or modified in an anomalous way.

Default severity: Low

- Feature: EKS audi

finding informs you that an anomalous API operation to create a `Role` or `ClusterRole` with excessive permissions was called by a Kubernetes user in your Amazon EKS cluster. Attackers can use role creation with powerful permissions to avoid

and avoid detection. The excessive permissions can lead to privileged escalation, remote code execution, and potentially control over a namespace or cluster. If this is not expected, it may indicate either a configuration mistake

compromised.

The observed API was identified as anomalous by the GuardDuty anomaly detection machine learning (ML) model. The ML model evaluates all user API activity within your Amazon EKS cluster and identifies

associated with the techniques used by unauthorized users. The ML model also tracks multiple factors of the API operation, such as the user making the request, the location the request was made from, the user agent used,

account, and the namespace that the user operated. You can find the details of the API request that are unusual, in the finding details panel in the GuardDuty console.

Remediation recommendations:

Examine the permissions defined

to ensure that all the permissions are needed and follow least privilege principles. If the permissions were granted mistakenly or maliciously, revoke user access and changes made by an unauthorized user to your cluster.

ting EKS Protection findings.

If your AWS credentials are compromised, see Remediating potentially compromised AWS credentials.

sion Chec ked

A user check ed their access permi ssion in an anom alous way.

Default severity : Low

- Feat ure: EKS audi t logs

This finding informs you that

cluster successfully checked whether or not the known powerful permissions that can lead to privileged escalation and remote code execution, are allowed. For example, command used to check permissions for a user is `kubectl auth`

expected, it may indicate either a configuration mistake or that your credentials have been compromised.

The observed API was identified as anomalous by the GuardDuty anomaly detection machine learning (ML) model. The ML model

within your Amazon EKS cluster and identifies anomalous events that are associated with the techniques used by unauthorized users. The ML model also [illegible] factors of the API operation, such as the user making

	the request was made from, permission being checked, and the namespace that the user operated. You can find the details of the API request that are unusual, in the finding details panel in the GuardDuty console.
	Remediation recomm

the permissions granted to the Kubernetes user to ensure that all the permissions are needed. If the permissions were granted mistakenly or maliciously, revoke user access and reverse any changes made by an unauthorized user to

ion, see Remediating EKS Protection findings.

If your AWS credentials are compromised, see Remediating potentially compromised AWS credentials.

Next topic: Runtime Monitoring finding types

Previous topic: S3 Protection finding types

Need help?

- Try AWS re:Post
- Connect with an AWS IQ expert