Kubernetes API Abuse (version 1.0)

**Cloud Service Label: IaaS, PaaS**

Description

Cloud workloads are becoming more and more dependent on Kubernetes. Kubernetes is a complex piece of software with a rich and complex API that can be exposed inadvertently through simple misconfigurations. Even when not misconfigured, it can still introduce access opportunities for attackers. In 2018 (CVE-2018-1002105), the first major vulnerability was reported that could compromise the integrity of an entire Kubernetes cluster due to a flaw in the Kubernetes API. Since then several other flaws have been discovered within the Kubernetes API with varying degrees of severity. The remediation in every case has been to upgrade Kubernetes to the latest version. This however may become more problematic as more cloud workloads rely on Kubernetes clusters to handle workloads with strict uptime requirements. If past is prologue, new critical API vulnerabilities can be expected in the coming years. Similar to the Kubernetes API but distinct is the Kubectl command line utility that can also control a Kubernetes cluster. Key vulnerabilities have begun to be found in this software also that could enable an adversary with some cloud console access to increase his capabilities.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| CVE-2019-1002101 | Allowed adversaries to inject random code running at the privileges of a container if they could simply replace the tar binary in any running container with an executable named tar. |

Mitigations

|  |  |
| --- | --- |
| **Mitigation** | **Description** |
| Limit API Server Access | Ensure the API server is accessible only from trusted subnets in a Virtual network. |
| No Anonymous Authentication | Ensure that anonymous authentication is disabled. |
| Periodic Vulnerability Scanning | Periodically use a Kubernetes vulnerability scanner on any Kubernetes clusters deployed on IaaS. |

Detection

Monitor Kubernetes cluster activity to locate unexplained stoppage and starting of containers which could be indicative of adversary experimentation utilizing the Kubernetes API.

|  |  |
| --- | --- |
| **Detection** | **Description** |
| Create Log Metric Filters and Alarms for AWS | To create a metric filter and alarm:   1. Create a metric filter that checks for IAM policy changes and the *<cloudtrail\_log\_group\_name>* 2. Create an SNS topic 3. Create an SNS subscription to the above topic 4. Create an alarm associated with the filter and SNS topic created in steps 1 and 2 respectively |
| Monitor Activity in AWS Account | Various services in AWS offer logging features that allow for detection capabilities. These include CloudFront, CloudTrail, CloudWatch, Config, and S3. |
| Monitor for Suspicious Activity in Azure | Azure AD can generate anomaly reports than can be run on a daily basis. Azure AD Identity Protection show current risks in its dashboard and provides daily email summary notifications. Policies can also be configured to alert to specific issues. |
| Create Log Metric Filters and Alarms for CloudTrail | To create a metric filter and alarm:   1. Create a filter that checks for CloudTrail changes and the specific *<cloudtrail\_log\_group\_name>* 2. Create an SNS topic that the alarm will notify 3. Create an SNS subscription to the above topic 4. Create an alarm associated with the filter from step 1 and SNS topic in step 2 |
| Create Activity Log Alerts in Azure | To create log activity alerts for deletion in the Azure Console:   1. Navigate to *Monitor’ / ‘Alerts* 2. Select *Manage alert rules* 3. Click on the Alert *Name* where Condition contains *operationName equals Microsoft.Network/networkSecurityGroups/securityRules/delete* 4. Hover a mouse over *Condition* to ensure it is set to *Whenever the Administrative Activity Log “Delete Security Rule (networkSecurityGroups/securityRules)” has “any” level with “any” status and event is initiated by “any*” |
| Create, View, and Manage Activity Alerts in Azure Monitor | To create a log alert in the Azure portal:   1. Select **Monitor -> Alerts** 2. Select **New alert rule** of the **Alerts** window 3. Provide information in **Define alert condition** 4. Provide details in **Define alert details** 5. Specify action group for new alert rule under **Action group**, or create a new action group with + **New group** 6. Select **Yes** for the **Enable rule upon creation** option 7. Select **Create alert rule**   To view and manage alerts:   1. Select **Monitor -> Alerts -> Manage alert rules** 2. Select the rule you want to modify and double-click to edit the rule options 3. Click **Save** |
| Azure Resource Manager Templates | Azure Resource Manager templates in the format of JSON files that can be used to configure metric alerts in Azure Monitor. These templates can be used for simple static and dynamic threshold metric alerts, availability tests, and monitoring multiple resources. |
| Enable CloudTrail across all regions in AWS | To enable CloudTrail across all regions:   1. Sign into the AWS Management Console and open the CloudTrail console 2. Click on *Trails* 3. Set necessary Trails to All option in the I column 4. Click on a trail via the link *Name* column 5. Set *Logging* to *ON* 6. Set *Apply trail to all regions* to *Yes* |
| Configure log profile to capture activity logs for all regions in Azure | To set up activity logs for all regions:   1. Navigate to Azure console 2. Go to *Activity log* 3. Select *Export* 4. Select *Subscription* 5. Check *Select all* in *Regions* 6. Select *Save* |

References

1. <https://www.stackrox.com/post/2020/01/top-5-kubernetes-vulnerabilities-of-2019-the-year-in-review/> - Accessed March 8,2020
2. https://arstechnica.com/information-technology/2018/02/tesla-cloud-resources-are-hacked-to-run-cryptocurrency-mining-malware – Accessed March 8, 2020
3. <https://github.com/aquasecurity/kube-hunter> - Accessed March 8, 2020