Secrets
ABAP
Apex
C
C++
CloudFormation
COBOL
C#
CSS
Flex
Go
HTML
Java
JavaScript
Kotlin
Kubernetes
Objective C
PHP
PL/I
PL/SQL
Python
RPG
Ruby
Scala
Swift
Terraform
Text
TypeScript
T-SQL
VB.NET
VB6
XML

CloudFormation static code analysis

Unique rules to find Bugs, Vulnerabilities, Security Hotspots, and Code Smells in your CLOUDFORMATION code

All rules 27 | Vulnerability 3 | Security Hotspot 20 | Code Smell 4

Tags | Search by name...

Security Hotspot

Using unencrypted SNS topics is security-sensitive
Security Hotspot

Using unencrypted SageMaker notebook instances is security-sensitive
Security Hotspot

Using unencrypted Elasticsearch domains is security-sensitive
Security Hotspot

Using unencrypted RDS databases is security-sensitive
Security Hotspot

Using unencrypted EBS volumes is security-sensitive
Security Hotspot

Disabling logging is security-sensitive
Security Hotspot

"Log Groups" should be declared explicitly
Code Smell

Administration services access should be restricted to specific IP addresses
Vulnerability

Disabling versioning of S3 buckets is security-sensitive
Security Hotspot

Disabling server-side encryption of S3 buckets is security-sensitive
Security Hotspot

AWS tag keys should comply with a naming convention
Code Smell

CloudFormation parsing failure
Code Smell

Administration services access should be restricted to specific IP addresses

Vulnerability | Minor | cwe owasp aws

Analyze your code

Cloud platforms such as AWS, Azure, or GCP support virtual firewalls that can be used to restrict access to services by controlling inbound and outbound traffic.
Any firewall rule allowing traffic from all IP addresses to standard network ports on which administration services traditionally listen, such as 22 for SSH, can expose these services to exploits and unauthorized access.

Recommended Secure Coding Practices

It's recommended to restrict access to remote administration services to only trusted IP addresses. In practice, trusted IP addresses are those held by system administrators or those of bastion-like servers.

Noncompliant Code Example

An ingress rule allowing all inbound SSH traffic:

```
MySecurityGroup:
    Type: "AWS::EC2::SecurityGroup"
    Properties:
      GroupDescription: "noncompliant"
      VpcId: !Ref myVPC
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 22
          ToPort: 22 # SSH traffic
          CidrIp: "0.0.0.0/0" # from all IP addresses is authorized
```

Compliant Solution

An ingress rule allowing inbound SSH traffic from specific IP addresses:

```
MySecurityGroup:
    Type: "AWS::EC2::SecurityGroup"
    Properties:
      GroupDescription: "compliant"
      VpcId: !Ref myVPC
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 22
          ToPort: 22
          CidrIp: "1.2.3.0/24"
```

See

- MITRE, CWE-284 - Improper Access Control
- OWASP Top 10 2017 Category A5 - Broken Access Control
- OWASP Top 10 2021 Category A1 - Broken Access Control
- AWS Documentation - Security groups for your VPC
- Azure Documentation - Network security groups
- GCP Documentation - Firewalls

Available In:

sonarcloud | sonarqube