


































-  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

Allowing public network access to cloud resources is security-sensitive		Security Hotspot
Having AWS policies that grant access to all resources of an account is security-sensitive		Security Hotspot
Having policies that grant all privileges is security-sensitive		Security Hotspot
Policies authorizing public access to resources are security-sensitive		Security Hotspot
Granting access to S3 buckets to all or authenticated users is security-sensitive		Security Hotspot
AWS IAM policies should not allow privilege escalation		Vulnerability
Weak SSL/TLS protocols should not be used		Vulnerability
Allowing public ACLs or policies on a S3 bucket is security-sensitive		Security Hotspot
Authorizing HTTP communications with S3 buckets is security-sensitive		Security Hotspot
Using clear-text protocols is security-sensitive		Security Hotspot
"Log Groups" should be configured with a retention policy		Code Smell
Defining a short backup retention duration is security-sensitive		Security Hotspot

Allowing public network access to cloud resources is security-sensitive

Analyze your code

 Security Hotspot

 Blocker



 cwe

 owasp

 aws

Enabling public network access to cloud resources can affect an organization's ability to protect its data or internal operations from data theft or disruption.

Depending on the component, inbound access from the Internet can be enabled via:

- a boolean value that explicitly allows access to the public network.
- the assignment of a public IP address.
- database firewall rules that allow public IP ranges.

Deciding to allow public access may happen for various reasons such as for quick maintenance, time saving, or by accident.

This decision increases the likelihood of attacks on the organization, such as:

- data breaches.
- intrusions into the infrastructure to permanently steal from it.
- and various malicious traffic, such as DDoS attacks.

Ask Yourself Whether

This cloud resource:

- should be publicly accessible to any Internet user.
- requires inbound traffic from the Internet to function properly.

There is a risk if you answered no to any of those questions.

Recommended Secure Coding Practices

Avoid publishing cloud services on the Internet unless they are intended to be publicly accessible, such as customer portals or e-commerce sites.

Use private networks (and associated private IP addresses) and VPC peering or other secure communication tunnels to communicate with other cloud components.

The goal is to prevent the component from intercepting traffic coming in via the public IP address. If the cloud resource does not support the absence of a public IP address, assign a public IP address to it, but do not create listeners for the public IP address.

Noncompliant Code Example

DMS and EC2 instances have a public IP address assigned to them:

```
DMSInstance:
  Type: AWS::DMS::ReplicationInstance
  Properties:
    PubliclyAccessible: true # sensitive, by default it's also set to true

EC2Instance:
  Type: AWS::EC2::Instance
  Properties:
    NetworkInterfaces:
      - AssociatePublicIpAddress: true # sensitive, by default it's also set to true
        DeviceIndex: "0"
```

Compliant Solution

DMS and EC2 instances doesn't have a public IP address:

```
DMSInstance:
  Type: AWS::DMS::ReplicationInstance
  Properties:
    PubliclyAccessible: false

EC2Instance:
  Type: AWS::EC2::Instance
  Properties:
    NetworkInterfaces:
      - AssociatePublicIpAddress: false
        DeviceIndex: "0"
```

See

- [OWASP Top 10 2021 Category A1](#) - Broken Access Control
- [AWS Documentation](#) - Amazon EC2 instance IP addressing
- [AWS Documentation](#) - Public and private replication instances
- [AWS Documentation](#) - VPC Peering
- [MITRE, CWE-284](#) - Improper Access Control
- [MITRE, CWE-668](#) - Exposure of Resource to Wrong Sphere
- [OWASP Top 10 2017 Category A5](#) - Broken Access Control

Available In:

 | 