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...

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

Using unencrypted EFS file systems is security-sensitive
Security Hotspot

Using unencrypted SQS queues is security-sensitive
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

Weak SSL/TLS protocols should not be used

Analyze your code

Vulnerability Critical aws cwe privacy owasp sans-top25

This rule raises an issue when an insecure TLS protocol version (i.e. a protocol different from "TLSv1.2", "TLSv1.3", "DTLSv1.2", or "DTLSv1.3") is used or allowed.

It is recommended to enforce TLS 1.2 as the minimum protocol version and to disallow older versions like TLS 1.0. Failure to do so could open the door to downgrade attacks: a malicious actor who is able to intercept the connection could modify the requested protocol version and downgrade it to a less secure version.

See

- OWASP Top 10 2021 Category A2 - Cryptographic Failures
- OWASP Top 10 2021 Category A7 - Identification and Authentication Failures
- OWASP Top 10 2017 Category A3 - Sensitive Data Exposure
- OWASP Top 10 2017 Category A6 - Security Misconfiguration
- Mobile AppSec Verification Standard - Network Communication Requirements
- OWASP Mobile Top 10 2016 Category M3 - Insecure Communication
- MITRE, CWE-327 - Inadequate Encryption Strength
- MITRE, CWE-326 - Use of a Broken or Risky Cryptographic Algorithm
- SANS Top 25 - Porous Defenses
- SSL and TLS Deployment Best Practices - Use secure protocols

Noncompliant Code Example

For Amazon OpenSearch domains:

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  Example:
    Type: AWS::OpenSearchService::Domain
    Properties:
      DomainName: example
      DomainEndpointOptions:
        EnforceHTTPS: true
        TLSSecurityPolicy: "Policy-Min-TLS-1-0-2019-07"  # Noncompliant
```

For Amazon API Gateway:

```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  CustomApi:
    Type: AWS::ApiGateway::DomainName
    Properties:
      SecurityPolicy: "TLS_1_0"  # Noncompliant
```

```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  CustomApi: # Noncompliant
    Type: AWS::ApiGatewayV2::DomainName
```

Compliant Solution

For Amazon OpenSearch domains:

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  Example:
    Type: AWS::OpenSearchService::Domain
    Properties:
      DomainName: example
      DomainEndpointOptions:
        EnforceHTTPS: true
        TLSSecurityPolicy: "Policy-Min-TLS-1-2-2019-07"
```

For Amazon API Gateway:

```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  CustomApi:
    Type: AWS::ApiGateway::DomainName
    Properties:
      SecurityPolicy: "TLS_1_2"
```

```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  CustomApi:
    Type: AWS::ApiGatewayV2::DomainName
    Properties:
      DomainNameConfigurations:
        - SecurityPolicy: "TLS_1_2"
```

See

- OWASP Top 10 2021 Category A2 - Cryptographic Failures
- OWASP Top 10 2021 Category A7 - Identification and Authentication Failures
- OWASP Top 10 2017 Category A3 - Sensitive Data Exposure
- OWASP Top 10 2017 Category A6 - Security Misconfiguration
- Mobile AppSec Verification Standard - Network Communication Requirements
- OWASP Mobile Top 10 2016 Category M3 - Insecure Communication
- MITRE, CWE-327 - Inadequate Encryption Strength
- MITRE, CWE-326 - Use of a Broken or Risky Cryptographic Algorithm
- SANS Top 25 - Porous Defenses
- SSL and TLS Deployment Best Practices - Use secure protocols
- Amazon API Gateway - Choosing a minimum TLS version

Available In:

sonarcloud | sonarqube