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...

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
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

Using clear-text protocols is security-sensitive

Analyze your code

Security Hotspot | Critical | aws cwe owasp

Clear-text protocols such as `ftp`, `telnet` or non-secure `http` lack encryption of transported data, as well as the capability to build an authenticated connection. It means that an attacker able to sniff traffic from the network can read, modify or corrupt the transported content. These protocols are not secure as they expose applications to an extensive range of risks:

- Sensitive data exposure
- Traffic redirected to a malicious endpoint
- Malware infected software update or installer
- Execution of client side code
- Corruption of critical information

Even in the context of isolated networks like offline environments or segmented cloud environments, the insider threat exists. Thus, attacks involving communications being sniffed or tampered with can still happen.

For example, attackers could successfully compromise prior security layers by:

- Bypassing isolation mechanisms
- Compromising a component of the network
- Getting the credentials of an internal IAM account (either from a service account or an actual person)

In such cases, encrypting communications would decrease the chances of attackers to successfully leak data or steal credentials from other network components. By layering various security practices (segmentation and encryption, for example), the application will follow the *defense-in-depth* principle.

Note that using the `http` protocol is being deprecated by major web browsers.

In the past, it has led to the following vulnerabilities:

- CVE-2019-6169
- CVE-2019-12327
- CVE-2019-11065

Ask Yourself Whether

- Application data needs to be protected against falsifications or leaks when transiting over the network.
- Application data transits over a network that is considered untrusted.
- Compliance rules require the service to encrypt data in transit.
- Your application renders web pages with a relaxed mixed content policy.
- OS level protections against clear-text traffic are deactivated.

There is a risk if you answered yes to any of those questions.

Recommended Secure Coding Practices

- Make application data transit over a secure, authenticated and encrypted protocol like TLS or SSH. Here are a few alternatives to the most common clear-text protocols:
  - Use `ssh` as an alternative to `telnet`
  - Use `sftp`, `scp` or `ftps` instead of `ftp`
  - Use `https` instead of `http`
  - Use `SMTP` over `SSL`/`TLS` or `SMTP` with `STARTTLS` instead of clear-text SMTP
- Enable encryption of cloud components communications whenever it's possible.
- Configure your application to block mixed content when rendering web pages.
- If available, enforce OS level deativation of all clear-text traffic

It is recommended to secure all transport channels (even local network) as it can take a single non secure connection to compromise an entire application or system.

Sensitive Code Example

For AWS Kinesis Data Streams, server-side encryption is disabled by default:

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  KinesisStream: # Sensitive
    Type: AWS::Kinesis::Stream
    Properties:
      ShardCount: 1
    # No StreamEncryption
```

For Amazon ElastiCache:

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  Example:
    Type: AWS::ElastiCache::ReplicationGroup
    Properties:
      ReplicationGroupId: "example"
      TransitEncryptionEnabled: false  # Sensitive
```

For Amazon ECS:

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  EcsTask:
    Type: AWS::ECS::TaskDefinition
    Properties:
      Family: "service"
      Volumes:
        -
          Name: "storage"
          EFSVolumeConfiguration:
            FilesystemId: !Ref FS
            TransitEncryption: "DISABLED"  # Sensitive
```

For AWS Load Balancer Listeners:

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  HTTPListener:
    Type: "AWS::ElasticLoadBalancingV2::Listener"
    Properties:
      DefaultActions:
        - Type: "redirect"
          RedirectConfig:
            Protocol: "HTTP"
      Protocol: "HTTP" # Sensitive
```

For Amazon OpenSearch domains:

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  Example:
    Type: AWS::OpenSearchService::Domain
    Properties:
      DomainName: example
      DomainEndpointOptions:
        EnforceHTTPS: false # Sensitive
      NodeToNodeEncryptionOptions:
        Enabled: false # Sensitive
```

For Amazon MSK communications between clients and brokers:

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  MSKCluster:
    Type: 'AWS::MSK::Cluster'
    Properties:
      ClusterName: MSKCluster
      EncryptionInfo:
        EncryptionInTransit:
          ClientBroker: TLS_PLAINTEXT # Sensitive
          InCluster: false # Sensitive
```

Compliant Solution

For AWS Kinesis Data Streams server-side encryption:

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  KinesisStream:
    Type: AWS::Kinesis::Stream
    Properties:
      ShardCount: 1
      StreamEncryption:
        EncryptionType: KMS
```

For Amazon ElastiCache:

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  Example:
    Type: AWS::ElastiCache::ReplicationGroup
    Properties:
      ReplicationGroupId: "example"
      TransitEncryptionEnabled: true
```

For Amazon ECS:

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  EcsTask:
    Type: AWS::ECS::TaskDefinition
    Properties:
      Family: "service"
      Volumes:
        -
          Name: "storage"
          EFSVolumeConfiguration:
            FilesystemId: !Ref FS
            TransitEncryption: "ENABLED"
```

For AWS Load Balancer Listeners:

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  HTTPListener:
    Type: "AWS::ElasticLoadBalancingV2::Listener"
    Properties:
      DefaultActions:
        - Type: "redirect"
          RedirectConfig:
            Protocol: "HTTPS"
      Protocol: "HTTP"
```

For Amazon OpenSearch domains:

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  Example:
    Type: AWS::OpenSearchService::Domain
    Properties:
      DomainName: example
      DomainEndpointOptions:
        EnforceHTTPS: true
      NodeToNodeEncryptionOptions:
        Enabled: true
```

For Amazon MSK communications between clients and brokers, data in transit is encrypted by default, allowing you to omit writing the `EncryptionInTransit` configuration. However, if you need to configure it explicitly, this configuration is compliant:

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  MSKCluster:
    Type: 'AWS::MSK::Cluster'
    Properties:
      ClusterName: MSKCluster
      EncryptionInfo:
        EncryptionInTransit:
          ClientBroker: TLS
          InCluster: true
```

See

- OWASP Top 10 2021 Category A2 - Cryptographic Failures
- OWASP Top 10 2017 Category A3 - Sensitive Data Exposure
- Mobile AppSec Verification Standard - Network Communication Requirements
- OWASP Mobile Top 10 2016 Category M3 - Insecure Communication
- MITRE, CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
- MITRE, CWE-319 - Cleartext Transmission of Sensitive Information
- Google, Moving towards more secure web
- Mozilla, Deprecating non secure http

Available In:

sonarcloud | sonarqube