

Secrets

ABAP

Apex

C

C++

CloudFormation

COBOL

C#

CSS

Flex

Go

HTML

Java

JavaScript

Kotlin

Objective C

PHP

PL/I

PL/SQL

Python

RPG

Ruby

Scala

Swift

Terraform

Text

TypeScript

T-SQL

VB.NET

VB6

XML

Terraform static code analysis

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

All rules50

Vulnerability5

Security Hotspot43

Code Smell2

Tags

Search by name...

Security Hotspot

Using unencrypted EFS file systems is security-sensitive

Security Hotspot

Security Hotspot

Using unencrypted SQS queues is security-sensitive

Security Hotspot

Security Hotspot

Using unencrypted SNS topics is security-sensitive

Security Hotspot

Security Hotspot

Using unencrypted SageMaker notebook instances is security-sensitive

Security Hotspot

Security Hotspot

Using unencrypted Elasticsearch domains is security-sensitive

Security Hotspot

Security Hotspot

Using unencrypted RDS databases is security-sensitive

Security Hotspot

Security Hotspot

Using unencrypted EBS volumes is security-sensitive

Security Hotspot

Security Hotspot

Disabling logging is security-sensitive

Security Hotspot

Vulnerability

Administration services access should be restricted to specific IP addresses

Vulnerability

Security Hotspot

Unversioned Google Cloud Storage buckets are security-sensitive

Security Hotspot

Security Hotspot

Disabling S3 bucket MFA delete is security-sensitive

Security Hotspot

Disabling certificate-based authentication is security-sensitive

Analyze your code

Security Hotspot

Major

cwe owasp azure

Disabling certificate-based authentication can reduce an organization's ability to react against attacks on its critical functions and data if any.

Azure offers various authentication options to access resources: Anonymous connections, Basic authentication, password-based authentication, and certificate-based authentication.

Choosing certificate-based authentication helps bring client/host trust by allowing the host to verify the client and vice versa. In case of a security incident, certificates help bring investigators traceability and allow security operations teams to react faster (by massively revoking certificates, for example).

Ask Yourself Whether

This Azure resource is essential for the information system infrastructure.

This Azure resource is essential for mission-critical functions.

Compliance policies require access to this resource to be authenticated with certificates.

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

Recommended Secure Coding Practices

Enable certificate-based authentication.

Sensitive Code Example

For App Service:

resource "azurerm_app_service" "example" { client_cert_enabled = false # Sensitive }

For Logic App Standards and Function Apps:






resource "azurerm_function_app" "example" { client_cert_mode = "Optional" # Sensitive }

For Data Factory Linked Services:

resource "azurerm_data_factory_linked_service_web" "example" { authentication_type = "Basic" # Sensitive }

https://rules.sonarsource.com/terraform/RSPEC-6382

1/2

 Security Hotspot
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
Terraform parsing failure  Code Smell

For [API Management](#):

```
resource "azurerm_api_management" "example" {
  sku_name = "Consumption_1"
  client_certificate_mode = "Optional" # Sensitive
}
```

For [Linux and Windows Web Apps](#):

```
resource "azurerm_linux_web_app" "example" {
  client_cert_enabled = false # Sensitive
}
resource "azurerm_linux_web_app" "exemple2" {
  client_cert_enabled = true
  client_cert_mode = "Optional" # Sensitive
}
```

Compliant Solution

For [App Service](#):

```
resource "azurerm_app_service" "example" {
  client_cert_enabled = true
}
```

For [Logic App Standards](#) and [Function Apps](#):

```
resource "azurerm_function_app" "example" {
  client_cert_mode = "Required"
}
```

For [Data Factory Linked Services](#):

```
resource "azurerm_data_factory_linked_service_web" "example" {
  authentication_type = "ClientCertificate"
}
```

For [API Management](#):

```
resource "azurerm_api_management" "example" {
  sku_name = "Consumption_1"
  client_certificate_mode = "Required"
}
```

For [Linux and Windows Web Apps](#):

```
resource "azurerm_linux_web_app" "example" {
  client_cert_enabled = true
  client_cert_mode = "Required"
}
```

See

- [OWASP Top 10 2021 Category A1](#) - Broken Access Control
- [OWASP Top 10 2017 Category A5](#) - Broken Access Control
- [MITRE, CWE-668](#) - Exposure of Resource to Wrong Sphere

Available In:

