components

For AWS:

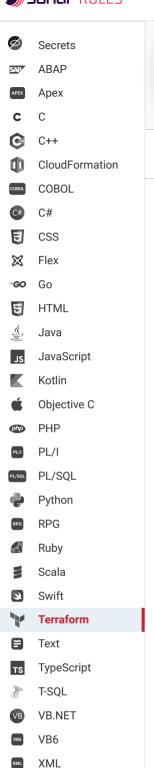
listeners for the public IP address.

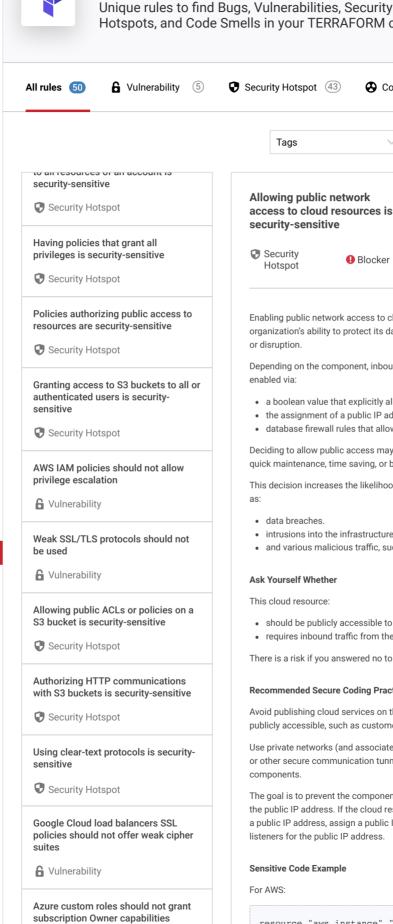
Sensitive Code Example

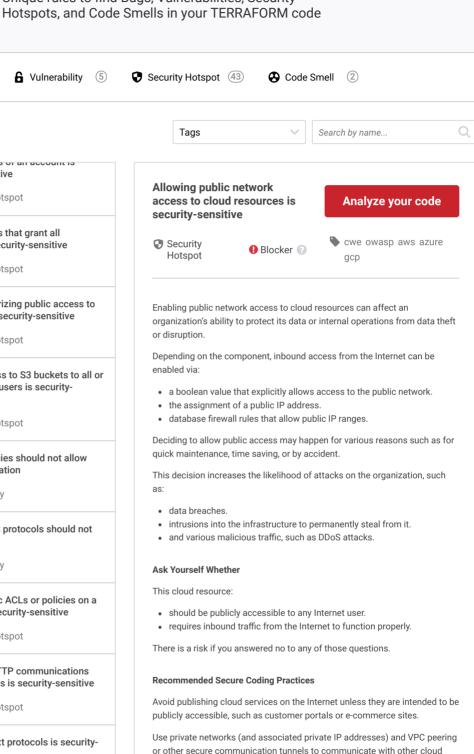
Terraform static code analysis



Products >







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

associate_public_ip_address = true # Sensitive

resource "aws_instance" "example" {

6 Vulnerability

Excluding users or groups activities from audit logs is security-sensitive

Security Hotspot

Defining a short log retention duration is security-sensitive

Security Hotspot

Enabling Attribute-Based Access Control for Kubernetes is securitysensitive

Security Hotspot

Creating custom roles allowing privilege escalation is securitysensitive

Security Hotspot

```
resource "aws_dms_replication_instance" "example" {
  publicly_accessible = true # Sensitive
}
```

For Azure:

```
resource "azurerm_postgresql_server" "example" {
   public_network_access_enabled = true # Sensitive
}
```

```
resource "azurerm_postgresql_server" "example" {
  public_network_access_enabled = true # Sensitive
}
```

```
resource "azurerm_kubernetes_cluster" "production" {
   api_server_authorized_ip_ranges = ["176.0.0.0/4"] # S
   default_node_pool {
     enable_node_public_ip = true # Sensitive
   }
}
```

For GCP:

```
resource "google_compute_instance" "example" {
  network_interface {
    network = "default"

    access_config { # Sensitive
    # Ephemeral public IP
    }
}
```

Compliant Solution

For AWS:

```
resource "aws_instance" "example" {
  associate_public_ip_address = false
}
```

```
resource "aws_dms_replication_instance" "example" {
  publicly_accessible = false
}
```

For Azure:

```
resource "azurerm_postgresql_server" "example" {
   public_network_access_enabled = false
}
```

```
resource "azurerm_kubernetes_cluster" "production" {
   api_server_authorized_ip_ranges = ["192.168.0.0/16"]
   default_node_pool {
      enable_node_public_ip = false
   }
}
```

For GCP:

```
resource "google_compute_instance" "example" {
  network_interface {
    network = "default"
  }
}
```

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:

sonarcloud 👌 | sonarqube

© 2008-2022 SonarSource S.A., Switzerland. All content is copyright protected. SONAR, SONARSOURCE, SONARLINT, SONARQUBE and SONARCLOUD are trademarks of SonarSource S.A. All other trademarks and copyrights are the property of their respective owners. All rights are expressly reserved. Privacy Policy