




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 rules 50

Vulnerability 5

Security Hotspot 43

Code Smell 2

Tags ▾

Search by name... 🔍

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

Administration services access should be restricted to specific IP addresses

Vulnerability

Unversioned Google Cloud Storage buckets are security-sensitive

Security Hotspot

Disabling S3 bucket MFA delete is security-sensitive

Security Hotspot

Administration services access should be restricted to specific IP addresses

Analyze your code

Vulnerability Minor ⓘ cwe owasp aws azure gcp

Cloud platforms such as AWS, Azure, or GCP support virtual firewalls that can be used to restrict access to services by controlling inbound and outbound traffic.

Any firewall rule allowing traffic from all IP addresses to standard network ports on which administration services traditionally listen, such as 22 for SSH, can expose these services to exploits and unauthorized access.

Recommended Secure Coding Practices

It's recommended to restrict access to remote administration services to only trusted IP addresses. In practice, trusted IP addresses are those held by system administrators or those of [bastion-like](#) servers.

Noncompliant Code Example

An ingress rule allowing all inbound SSH traffic for AWS:

```
resource "aws_security_group" "noncompliant" {
  name      = "allow_ssh_noncompliant"
  description = "allow_ssh_noncompliant"
  vpc_id    = aws_vpc.main.id

  ingress {
    description = "SSH rule"
    from_port   = 22
    to_port     = 22
    protocol    = "tcp"
    cidr_blocks = ["0.0.0.0/0"] # Noncompliant
  }
}
```






A security rule allowing all inbound SSH traffic for Azure:

```
resource "azurerm_network_security_rule" "noncompliant" {
  priority      = 100
  direction    = "Inbound"
  access       = "Allow"
  protocol     = "Tcp"
  source_port_range = "*"
  destination_port_range = "22"
  source_address_prefix = "*" # Noncompliant
  destination_address_prefix = "*"
}
```

A firewall rule allowing all inbound SSH traffic for GCP:

https://rules.sonarsource.com/terraform/RSPEC-6321

1/3

| |
|---|
|  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 |

```
resource "google_compute_firewall" "noncompliant" {
  network = google_compute_network.default.name

  allow {
    protocol = "tcp"
    ports    = ["22"]
  }

  source_ranges = ["0.0.0.0/0"] # Noncompliant
}
```

A security rule allowing all inbound SSH traffic for Azure:

```
resource "azurerm_network_security_rule" "noncompliant" {
  priority          = 100
  direction         = "Inbound"
  access            = "Allow"
  protocol          = "Tcp"
  source_port_range = "*"
  destination_port_range = "22"
  source_address_prefix = "*" # Noncompliant
  destination_address_prefix = "*"
}
```

Compliant Solution

An ingress rule allowing inbound SSH traffic from specific IP addresses for AWS:

```
resource "aws_security_group" "compliant" {
  name        = "allow_ssh_compliant"
  description = "allow_ssh_compliant"
  vpc_id      = aws_vpc.main.id

  ingress {
    description = "SSH rule"
    from_port   = 22
    to_port     = 22
    protocol    = "tcp"
    cidr_blocks = ["1.2.3.0/24"]
  }
}
```

A security rule allowing inbound SSH traffic from specific IP addresses for Azure:

```
resource "azurerm_network_security_rule" "compliant" {
  priority          = 100
  direction         = "Inbound"
  access            = "Allow"
  protocol          = "Tcp"
  source_port_range = "*"
  destination_port_range = "22"
  source_address_prefix = "1.2.3.0"
  destination_address_prefix = "*"
}
```

A firewall rule allowing inbound SSH traffic from specific IP addresses for GCP:

```
resource "google_compute_firewall" "compliant" {
  network = google_compute_network.default.name

  allow {
    protocol = "tcp"
    ports    = ["22"]
  }

  source_ranges = ["10.0.0.1/32"]
}
```

See

- [MITRE, CWE-284](#) - Improper Access Control
- [OWASP Top 10 2017 Category A5](#) - Broken Access Control
- [OWASP Top 10 2021 Category A1](#) - Broken Access Control
- [AWS Documentation](#) - Security groups for your VPC
- [Azure Documentation](#) - Network security groups
- [GCP Documentation](#) - Firewalls

Available In:



© 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](#)