




 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... 


 Vulnerability


Azure custom roles should not grant subscription Owner capabilities




 Security Hotspot


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 security-sensitive




 Security Hotspot

Creating custom roles allowing privilege escalation is security-sensitive



 Security Hotspot

Creating App Engine handlers without requiring TLS is security-sensitive



 Security Hotspot

Excessive granting of GCP IAM permissions is security-sensitive

 Security Hotspot

Enabling project-wide SSH keys to access VM instances is security-sensitive

 Security Hotspot




Granting public access to GCP resources is security-sensitive

 Security Hotspot

Creating GCP SQL instances without requiring TLS is security-sensitive

AWS IAM policies should not allow privilege escalation

Analyze your code

 Vulnerability  Critical  cwe owasp aws

AWS Identity and Access Management (IAM) is the service that defines access to AWS resources. One of the core components of IAM is the policy which, when attached to an identity or a resource, defines its permissions. Policies granting permission to an Identity (a User, a Group or Role) are called identity-based policies. They add the ability to an identity to perform a predefined set of actions on a list of resources.

Here is an example of a policy document defining a limited set of permission that grants a user the ability to manage his own access keys.





```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "iam:CreateAccessKey",
        "iam:DeleteAccessKey",
        "iam:ListAccessKeys",
        "iam:UpdateAccessKey"
      ],
      "Resource": "arn:aws:iam::245500951992:user*",
      "Effect": "Allow",
      "Sid": "AllowManageOwnAccessKeys"
    }
  ]
}
```

Privilege escalation generally happens when an identity policy gives to an identity the ability to grant more privileges than the ones it already has. Here is another example of a policy document that hides a privilege escalation. It allows an identity to generate a new access key for any user from the account, including users with high privileges.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "iam:CreateAccessKey",
        "iam:DeleteAccessKey",
        "iam:ListAccessKeys",
        "iam:UpdateAccessKey"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "AllowManageOwnAccessKeys"
    }
  ]
}
```

https://rules.sonarsource.com/terraform/RSPEC-6317

1/3

Creating DNS zones without DNSSEC enabled is security-sensitive
 Security Hotspot
Creating keys without a rotation period is security-sensitive
 Security Hotspot
Granting highly privileged GCP resource rights is security-sensitive
 Security Hotspot
Using unencrypted cloud storages is security-sensitive
 Security Hotspot
Azure role assignments that grant access to all resources of a

```
    ]
  }
```

Although it looks like it grants a limited set of permissions, this policy would, in practice, give the highest privileges to the identity it's attached to.

Privilege escalation is a serious issue as it allows a malicious user to easily escalate to a high privilege identity from a low privilege identity it took control of.

The example above is just one of many permission combinations that the rule can detect. There are other variants based on `iam:PassRole`, `lambda:UpdateFunctionCode`, and other IAM permissions that allow to update, create, and attach IAM policies.

The general recommendation to protect against privilege escalation is to restrict the resources that are granted sensitive permissions to. The first example above is a good demonstration of sensitive permissions being used with a narrow scope of resources and where no privilege escalation is possible.

Noncompliant Code Example

This policy allows to update the code of any lambda function. Updating the code of a lambda executing with high privileges will lead to privilege escalation.

```
resource "aws_iam_policy" "lambdaUpdatePolicy" {
  name = "lambdaUpdatePolicy"
  policy =<<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lambda:UpdateFunctionCode"
      ],
      "Resource": "*"
    }
  ]
}
EOF
}
```

Compliant Solution

Narrow the policy to only allow to update the code of certain lambda functions.

```
resource "aws_iam_policy" "lambdaUpdatePolicy" {
  name = "lambdaUpdatePolicy"
  policy =<<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lambda:UpdateFunctionCode"
      ],
      "Resource": "arn:aws:lambda:us-east-2:12345"
    }
  ]
}
EOF
}
```

See

- [OWASP Top 10 2021 Category A1](#) - Broken Access Control
- [Rhino Security Labs](#) - AWS IAM Privilege Escalation – Methods and Mitigation
- [OWASP Top 10 2017 Category A5](#) - Broken Access Control
- [MITRE, CWE-269](#) - Improper Privilege Management

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](#)