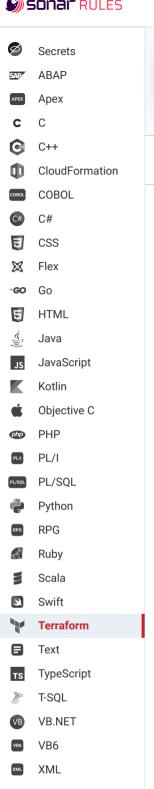
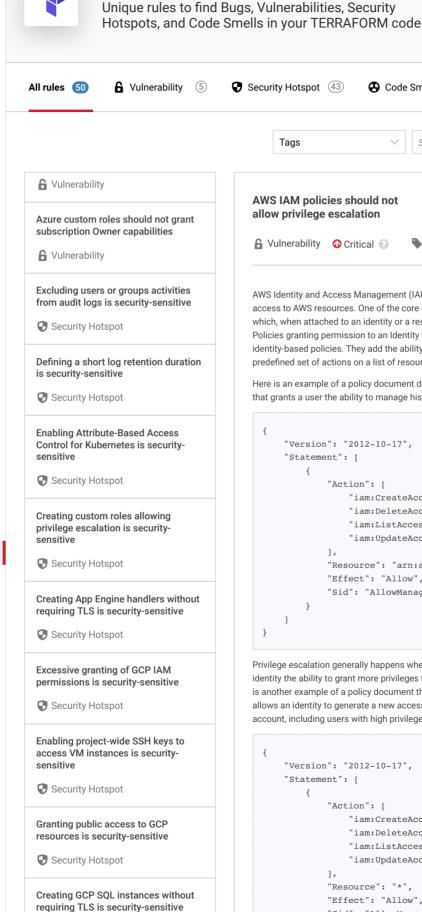
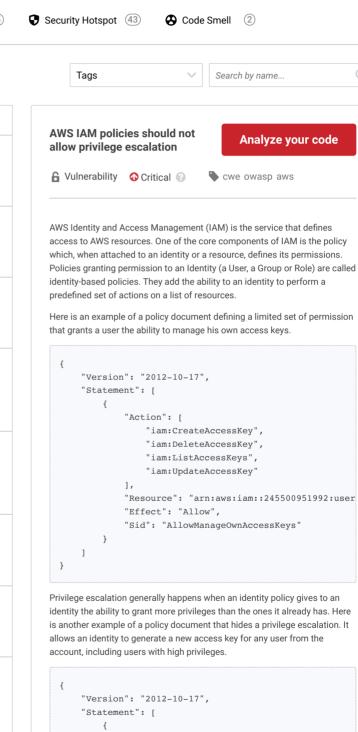
Terraform static code analysis



Products ∨







"Action": [

"Resource": "*",

"Effect": "Allow",

"iam:CreateAccessKey",

"iam:DeleteAccessKey",

"iam:ListAccessKeys",

"iam:UpdateAccessKey'

"Sid": "AllowManageOwnAccessKeys"

Security Hotspot

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.

Compliant Solution

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

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:
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