Checkmarx

KICS REPORT   v2.1.11

CRITICAL	0	HIGH	5	MEDIUM	21	LOW	0	INFO	9	TOTAL	35

PLATFORMS   Terraform, Common
START TIME   17:09:56, Jul 08 2025
END TIME   17:10:00, Jul 08 2025
SCANNED PATHS:
- /path

Google Storage Bucket Level Access Disabled   Results   4

Severity   HIGH
Platform   Terraform
Cwe   285
Category   Insecure Configurations

Description

Google Storage Bucket Level Access should be enabled

../../path/main.tf:605

Expected: google_storage_bucket[blog].uniform_bucket_level_access should be defined and not null

../../path/main.tf:25

Expected: google_storage_bucket[data_bucket].uniform_bucket_level_access should be defined and not null

../../path/main.tf:36

Expected: google_storage_bucket[dev_bucket].uniform_bucket_level_access should be defined and not null

../../path/main.tf:488

Expected: google_storage_bucket[function_bucket].uniform_bucket_level_access should be defined and not null

---

Passwords And Secrets - Generic Secret   Results   1

Severity   HIGH
Platform   Common
Cwe   798
Category   Secret Management

Description

Query to find passwords and secrets in infrastructure code.

../../path/main.tf:581

Expected: Hardcoded secret key should not appear in source

Cloud Storage Bucket Is Publicly Accessible   Results   4

Severity   MEDIUM
Platform   Terraform
Cwe   285
Category   Access Control

Description

Cloud Storage Bucket is anonymously or publicly accessible

../../path/main.tf:58

Expected: 'member' not equal to 'allUsers' nor 'allAuthenticatedUsers'

../../path/main.tf:634

Expected: 'member' not equal to 'allUsers' nor 'allAuthenticatedUsers'

../../path/main.tf:503

Expected: 'member' not equal to 'allUsers' nor 'allAuthenticatedUsers'

https://kics.io

KICS REPORT	v2.1.11

../../path/main.tf:72

Expected: 'member' not equal to 'allUsers' nor 'allAuthenticatedUsers'

🛡 Cloud Storage Bucket Logging Not Enabled

Results   **5**

Severity	MEDIUM
Platform	Terraform
Cwe	778
Category	Observability

Description

Cloud storage bucket should have logging enabled

../../path/main.tf:25

Expected: 'google_storage_bucket.logging' should be set

../../path/main.tf:36

Expected: 'google_storage_bucket.logging' should be set

../../path/main.tf:605

Expected: 'google_storage_bucket.logging' should be set

../../path/main.tf:683

Expected: 'google_storage_bucket.logging' should be set

../../path/main.tf:488

Expected: 'google_storage_bucket.logging' should be set

🛡 Cloud Storage Bucket Versioning Disabled

Results   **5**

Severity	MEDIUM
Platform	Terraform
Cwe	710
Category	Observability

Description

Cloud Storage Bucket should have versioning enabled

../../path/main.tf:25

Expected: 'versioning' should be defined and not null

../../path/main.tf:605

Expected: 'versioning' should be defined and not null

../../path/main.tf:683

Expected: 'versioning' should be defined and not null

../../path/main.tf:36

Expected: 'versioning' should be defined and not null

../../path/main.tf:488

Expected: 'versioning' should be defined and not null

🛡 Google Project Auto Create Network Disabled

Results   **1**

Severity	MEDIUM
Platform	Terraform
Cwe	799
Category	Insecure Configurations

Description

Verifies if the Google Project Auto Create Network is Disabled

https://kics.io

KICS REPORT   v2.1.11

../../path/main.tf:9

Expected: google_project[my_project].auto_create_network should be set to false

🛡 **Project-wide SSH Keys Are Enabled In VM Instances**   **Results**   **2**

Severity	MEDIUM
Platform	Terraform
Cwe	284
Category	Secret Management

Description

VM Instance should block project-wide SSH keys

../../path/main.tf:864

Expected: google_compute_instance[vm_instance_admin].metadata should be set

../../path/main.tf:812

Expected: google_compute_instance[vm_instance_public].metadata should be set

🛡 **SSH Access Is Not Restricted**   **Results**   **1**

Severity	MEDIUM
Platform	Terraform
Cwe	732
Category	Networking and Firewall

Description

Google Firewall should not allow SSH access (port 22) from the Internet (public CIDR block) to ensure the principle of least privileges

../../path/main.tf:768

Expected: 'google_compute_firewall[allow-ssh].allow.ports' should not include SSH port 22

🛡 **Service Account with Improper Privileges**   **Results**   **1**

Severity	MEDIUM
Platform	Terraform
Cwe	284
Category	Resource Management

Description

Service account should not have improper privileges like admin, editor, owner, or write roles

../../path/main.tf:858

Expected: google_project_iam_member[owner_binding].role should not have admin, editor, owner, or write privileges for service account member

🛡 **Using Default Service Account**   **Results**   **1**

Severity	MEDIUM
Platform	Terraform
Cwe	250
Category	Insecure Defaults

Description

Instances should not be configured to use the Default Service Account, that has full access to all Cloud APIs, which means the attribute 'service_account' and its sub attribute 'email' must be defined. Additionally, 'email' must not be empty and must also not be a default Google Compute Engine service account.

../../path/main.tf:829

KICS REPORT	**v2.1.11**

🛡 VM With Full Cloud Access

Results   **1**

Severity	MEDIUM
Platform	Terraform
Cwe	732
Category	Access Control

Description

A VM instance is configured to use the default service account with full access to all Cloud APIs

../../path/main.tf:881

Expected: 'service_account.scopes' should not contain 'cloud-platform'

🛡 Name Is Not Snake Case

Results   **7**

Severity	INFO
Platform	Terraform
Cwe	710
Category	Best Practices

Description

All names should follow snake case pattern.

../../path/main.tf:569

Expected: All names should be on snake case pattern

../../path/main.tf:594

Expected: All names should be on snake case pattern

../../path/main.tf:665

Expected: All names should be on snake case pattern

../../path/main.tf:762

Expected: All names should be on snake case pattern

../../path/main.tf:61

Expected: All names should be on snake case pattern

../../path/main.tf:47

Expected: All names should be on snake case pattern

../../path/main.tf:744

Expected: All names should be on snake case pattern

🛡 Output Without Description

Results   **1**

Severity	INFO
Platform	Terraform
Cwe	710
Category	Best Practices

Description

All outputs should contain a valid description.

../../path/main.tf:906

Expected: 'description' should be defined and not null

🛡 Variable Without Description

Results   **1**

Checkmarx

KICS REPORT   v2.1.11

Severity   INFO
Platform   Terraform
Cwe   710
Category   Best Practices

Description

All variables should contain a valid description.

../../path/main.tf:15
Expected: 'description' should be defined and not null