



# Cloud Infrastructure Audit For



Testers:

1. [REDACTED]
2. [REDACTED]
3. [REDACTED]

# Table of contents

|                                                                                                                       |          |
|-----------------------------------------------------------------------------------------------------------------------|----------|
| <b>Table of contents</b>                                                                                              | <b>2</b> |
| <b>Management Summary</b>                                                                                             | <b>4</b> |
| <b>Vulnerabilities by Risk</b>                                                                                        | <b>5</b> |
| <b>Approach</b>                                                                                                       | <b>6</b> |
| Scope Overview                                                                                                        | 6        |
| Scope Validation                                                                                                      | 6        |
| Threat Model                                                                                                          | 6        |
| Issue Table Description                                                                                               | 7        |
| <b>Security Assessment Findings</b>                                                                                   | <b>8</b> |
| IAM                                                                                                                   | 9        |
| Least Privilege Principle not Enforced                                                                                | 9        |
| IAM Members with Service Roles at the Project Level                                                                   | 13       |
| User-Managed Service Account Keys in use                                                                              | 15       |
| VPC                                                                                                                   | 17       |
| Unrestricted Inbound Access                                                                                           | 17       |
| Logging Disabled                                                                                                      | 19       |
| Default VPC Network In Use                                                                                            | 21       |
| Cloud SQL                                                                                                             | 22       |
| Database Instances with Public IPs                                                                                    | 22       |
| Encryption in Transit not Enforced                                                                                    | 24       |
| Log_error_verbosity Database Flag for Cloud SQL PostgreSQL Instance Is NOT Set to DEFAULT or Stricter                 | 26       |
| 'cloudsql.enable_pgaudit' Database Flag for each Cloud Sql Postgresql Instance Is Set to 'on' For Centralized Logging | 27       |
| Cloud SQL Database Instances are not Configured With Automated Backups                                                | 28       |
| Missing logging Flags                                                                                                 | 29       |
| Compute Engine                                                                                                        | 32       |
| Block Project-Wide SSH Keys feature disabled                                                                          | 32       |
| OS Patch Management not configured                                                                                    | 33       |
| 'Enable Connecting to Serial Ports' Is enabled for VM Instance                                                        | 34       |
| OS Login for GCP Projects disabled                                                                                    | 35       |
| Logging                                                                                                               | 36       |
| NO Log Metric Filter and Alerts                                                                                       | 36       |
| NO least one sink used to export copies of all the log entries                                                        | 38       |
| Publicly Accessible Resources                                                                                         | 39       |
| Uniform Bucket-Level Access for Cloud Storage Buckets                                                                 | 42       |
| Key Rotation Disabled                                                                                                 | 44       |
|                                                                                                                       | 2        |

|                                                           |          |
|-----------------------------------------------------------|----------|
| GCP Memorystore for Redis has AUTH disabled               | 46       |
| Encryption with Customer-Managed Keys                     | 47       |
| Google Cloud API Keys in use                              | 1        |
| Artifact Registry - Vulnerability Scanning not Configured | 1        |
| <b>Appendix A: Security Evaluation Fixes</b>              | <b>1</b> |

# Management Summary

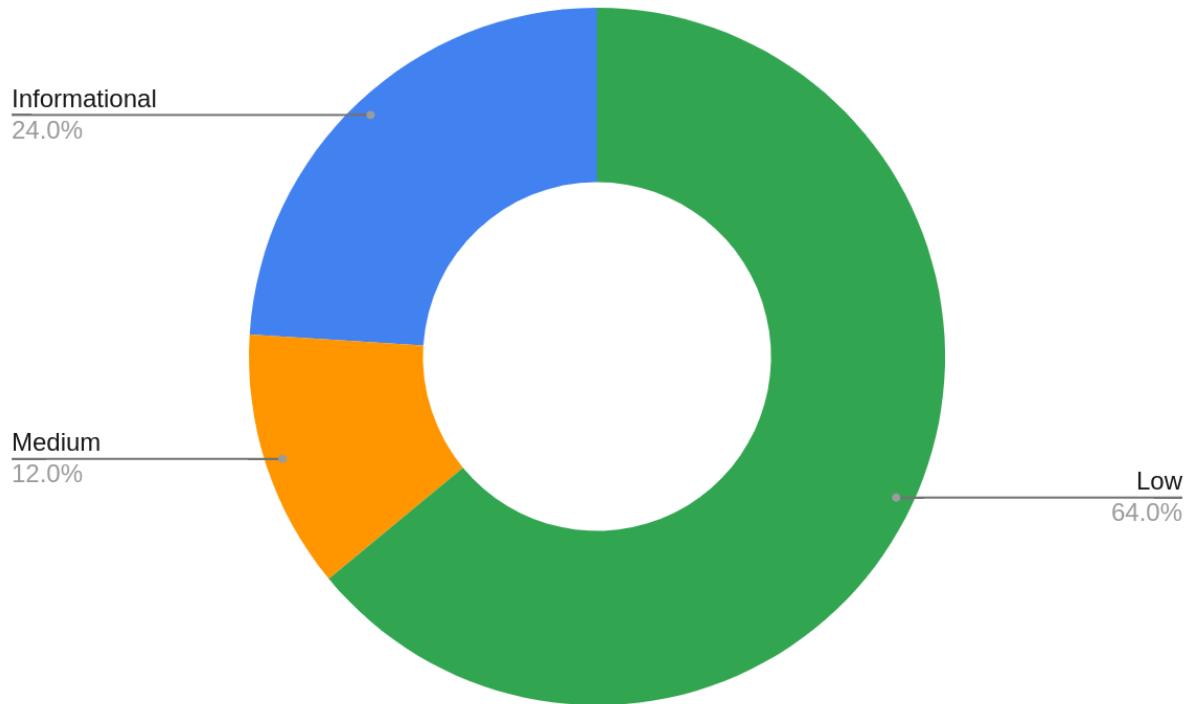
██████ contacted Sayfer Security in order to perform complete a cloud infrastructure audit on ██████ cloud infrastructure on 06/2023.

Before assessing the above services, we held a kickoff meeting with the ██████ technical team and received an overview of the system and the goals for this research.

We found a list of misconfigurations that we believe will increase the security of ██████.

Several fixes should be implemented following the report, but the system's security posture is competent.

## Vulnerabilities by Risk



| Risk        | Low | Medium | High | Informational |
|-------------|-----|--------|------|---------------|
| # of issues | 16  | 3      | 0    | 6             |

- **Low** – No direct threat exists. The vulnerability may be exploited using other vulnerabilities.
- **Medium** – Indirect threat to key business processes or partial threat to business processes.
- **High** – Direct threat to key business processes.
- **Informational** – This finding does not indicate vulnerability, but states a comment that notifies about design flaws and improper implementation that might cause a problem in the long run.

# Approach

## Scope Overview

During our first meeting and after understanding the company's needs, we defined the application's scope that resides at the following URLs as the scope of the project:

- [REDACTED]
- [REDACTED]
- [REDACTED]

Our tests were performed from 06/2022 to 07/2023.

## Scope Validation

We began by ensuring that the scope defined to us by the client was technically logical. Deciding what scope is right for a given system is part of the initial discussion. Getting the scope right is key to deriving maximum business value from the research.

## Threat Model

During our kickoff meetings with the client, we defined the most important assets the application possesses.

## Issue Table Description

### Issue title

|                    |                                                                                                                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location           | The URL in which this issue was detected. Issues with no location have no particular location and refer to the product as a whole.                                                                             |
| Risk               | Represents the risk factor of the issue. For further description refer to the Vulnerabilities by Risk section.                                                                                                 |
| Required Skill     | Describes the skill level required to conduct successful exploitation. The lower the skill level the easier the exploitation process.                                                                          |
| Affected services: | The services affected by the vulnerability.                                                                                                                                                                    |
| Description        | Here we provide a brief description of the issue and how it formed, the steps we made to find or exploit it, along with proof of concept (if present), and how this issue can affect the product or its users. |
| Mitigation         | Suggested resolving options for this issue and links to advised sites for further remediation.                                                                                                                 |

# Security Assessment Findings

## IAM

### Least Privilege Principle not Enforced

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location           | [REDACTED]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Risk               | Medium                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Required Skill     | High                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Affected services: | IAM                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Description        | <p>We have identified multiple Google Cloud identities that make use of Cloud IAM primitive roles, available within the GCP projects.</p> <p>Production:</p> <ul style="list-style-type: none"> <li>• [REDACTED] (Owner)</li> <li>• [REDACTED] (Editor)</li> <li>• [REDACTED] (Editor)</li> <li>• [REDACTED] (Editor)</li> <li>• [REDACTED] (Editor)</li> <li>• [REDACTED] (Editor)</li> <li>• [REDACTED] (Viewer)</li> <li>• [REDACTED] (Viewer)</li> </ul> <p>Following command can be used to verify it:</p> <pre>[REDACTED]</pre> <p>Cloud Identity and Access Management (IAM) service provides 3 types of roles:</p> <ul style="list-style-type: none"> <li>• primitive</li> <li>• predefined</li> <li>• custom roles</li> </ul> <p>Primitive roles, i.e. Owner, Editor and Viewer, are managed roles that existed prior to the introduction of Cloud IAM.</p> <p>Predefined roles are roles created and maintained by Google, that provide granular access to specific Google Cloud Platform resources and deny unwanted access to other resources.</p> <p>Custom roles are user-defined roles that allow you to bundle one or more supported permissions to meet your specific needs. Google Cloud projects are often (and overly) using primitive roles.</p> |

To implement the Principle of Least Privilege (POLP) and follow security best practices, grant predefined roles to IAM identities wherever possible, as these roles provide more granular access than the primitive roles. This eliminates over-privileged cloud identities from your Google Cloud projects and prevents any unwanted or unauthorized access to your GCP cloud resources.

### Privileged service accounts

We have also identified several service accounts that use privileged (administrator) roles:

Production:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Development:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Staging:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Following CLI commands can be used to verify it:

1.) Get service accounts with admin role:

```
[REDACTED]
```

2.) Get service accounts with Owner or Editor role:



As with all types of principals, you should only grant the service account the minimum set of permissions required to achieve its goal. When your Google Cloud Platform service accounts have administrator privileges (i.e. are using Owner and Editor roles, as well as roles containing \*Admin or \*admin in their names), these service accounts can access, create, and manage VM instances and other resources.

As an example, consider a service account that has a Storage Admin role assigned at the project level. It gives the service account access to all Cloud Storage buckets/objects in the project, including buckets/objects created in the future. In this way an attacker could also gain access to Cloud Storage buckets that contain sensitive data. In this situation, the service account is effectively as valuable as the Cloud Storage bucket itself: Instead of trying to access the bucket directly, a bad actor might attempt to take control of the service account. If that attempt is successful, the bad actor can escalate their privileges by impersonating the service account, which in turn gives them access to the sensitive information in the bucket.

To adhere to the principle of least privilege, give your GCP service accounts the minimal set of actions required to perform successfully their tasks and assigned the permissions/roles to the service accounts for a specific resource rather than assigning the permissions/roles at project level.

However, some of the above listed service accounts are Google-managed service accounts that are used to access the APIs of Google Cloud Platform services. These service accounts are designed specifically to run internal Google processes on your behalf and are owned by Google. By default, the account is automatically granted the project editor role on the project and is listed in the IAM section of Google Cloud console. However, you can change the roles granted to these service accounts, including revoking all access to your project.

To adhere to the principle of least privilege, use role recommendations to identify which permissions the service accounts are actually using, and which permissions might be unused. Adjust the allow policies of affected resources to help ensure that the service accounts aren't granted more access than they actually need. You should not modify Google-Managed service account's roles unless a role recommendation explicitly suggests that you modify them. More information can be found here: [https://cloud.google.com/compute/docs/access/service-accounts#google\\_apis\\_service\\_agent](https://cloud.google.com/compute/docs/access/service-accounts#google_apis_service_agent).

#### Mitigation

To implement the Principle of Least Privilege (POLP) and secure the access to your Google Cloud Platform (GCP) projects, revoke primitive roles, i.e. the Owner, Editor and Viewer, for each IAM identity (member) and attach one or more Cloud IAM predefined roles according to the identity access requirements.

The use of primitive roles should be limited to the following cases only:

- When the Google Cloud service does not provide a predefined role.
- When it is required to grant broader permissions for a GCP project (e.g. when granting permissions to development and/or test environments).

- When it is required to allow an IAM member to modify permissions for a GCP project. In this case, it is necessary to grant the identity the Owner role, because only owners have the permission to grant access to other IAM users.

We also recommend to give your GCP service accounts only the minimal set of actions required to perform successfully their tasks and remove any administrator-based roles that allows them overly permissive access.

More information can be found at:

<https://cloud.google.com/iam/docs/best-practices-for-securing-service-accounts>.

## IAM Members with Service Roles at the Project Level

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location           | [REDACTED]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Risk               | Medium                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Required Skill     | High                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Affected Services: | IAM                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Description        | <p>There are IAM members associated with Service Account User and/or Service Account Token Creator roles at the GCP project level:</p> <p><u>Production:</u></p> <p>Role: iam.serviceAccountTokenCreator</p> <p>Members:</p> <ul style="list-style-type: none"> <li>[REDACTED]</li> <li>[REDACTED]</li> <li>[REDACTED]</li> </ul> <p>Role: iam.serviceAccountUser</p> <p>Members:</p> <ul style="list-style-type: none"> <li>[REDACTED]</li> <li>[REDACTED]</li> </ul> <p><u>Development:</u></p> <p>Role: iam.serviceAccountTokenCreator</p> <p>Members:</p> <ul style="list-style-type: none"> <li>[REDACTED]</li> <li>[REDACTED]</li> <li>[REDACTED]</li> <li>[REDACTED]</li> <li>[REDACTED]</li> <li>[REDACTED]</li> <li>[REDACTED]</li> </ul> <p>Role: iam.serviceAccountUser</p> <p>Members</p> <ul style="list-style-type: none"> <li>[REDACTED]</li> <li>[REDACTED]</li> </ul> <p><u>Staging:</u></p> <p>Role: iam.serviceAccountTokenCreator</p> <p>Members:</p> <ul style="list-style-type: none"> <li>[REDACTED]</li> </ul> |

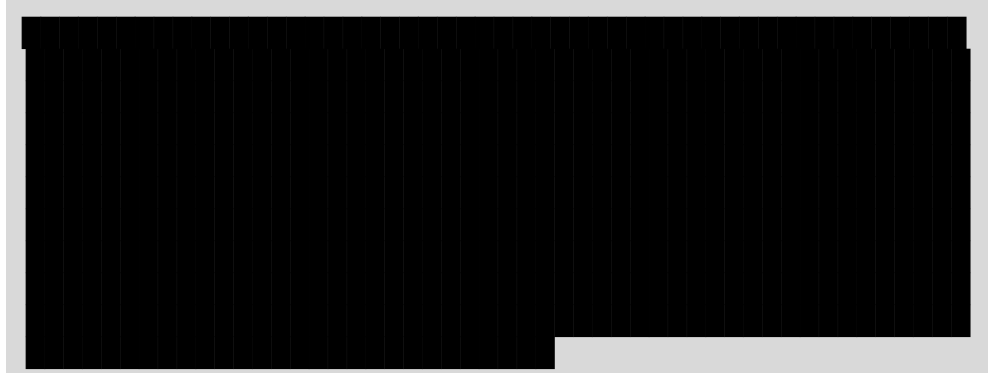
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Role: iam.serviceAccountUser

Members:

- [REDACTED]
- [REDACTED]

Following command can be used to verify it:



The Service Account User allows a principal to attach a service account to a resource. The Service Account Token Creator role allows a principal to directly impersonate, or assert, the identity of a service account.

Your organization may have multiple user-managed service accounts configured for a project. Granting the iam.serviceAccountUser or iam.serviceAccountTokenCreator roles to IAM principals for a project gives the principal access to all service accounts in the project, including service accounts created in the future. This can result in elevation of privileges.

To follow principle of least privilege and Google Cloud security best practices, IAM principals should not be assigned the Service Account User or Service Account Token Creator roles at the project level. These roles should be assigned to an IAM principals for a specific service account, giving that principal access to the service account.

#### Mitigation

We recommend implementing the principle of least privilege and assigning the Service Account User and Service Account Token Creator roles to IAM principals for a specific service account rather than assigning the role to a principal at project level.

More information can be found here:

- <https://cloud.google.com/iam/docs/best-practices-for-securing-service-accounts>
- <https://cloud.google.com/iam/docs/service-accounts#user-role>

## User-Managed Service Account Keys in use

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location           | [REDACTED]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Risk               | Low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Required Skill     | High                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Affected Services: | IAM                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Description        | <p>We have identified that the following Google Cloud Platform user-managed serviceaccount is using user-managed keys instead of GCP-managed keys for authentication:</p> <p>Production:</p> <ul style="list-style-type: none"> <li>• [REDACTED]</li> </ul> <p>Development:</p> <ul style="list-style-type: none"> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> </ul> <p>Staging:</p> <ul style="list-style-type: none"> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> </ul> <p>Following command can be used to verify it:</p> <pre>[REDACTED]</pre> <p>Anyone who has access to your user-managed keys will be able to access GCP resources through their associated service accounts. Deleting unwanted user-managed service account keys will significantly reduce the chances that a compromised set of keys can be used without your knowledge to access certain Google Cloud components and resources.</p> <p>Additionally, User-managed keys for all accounts mentioned above were not rotated over the last 90 days (334 days ago). Service Account keys should be rotated to ensure that data cannot be accessed with an old key that might have been lost, cracked, or stolen.</p> |

#### Mitigation

Avoid downloading service account keys and instead use the Workload Identity Federation if possible. Delete any user-managed keys associated with your Google Cloud Platform (GCP) service accounts.

In some scenarios, you may encounter circumstances where it is not possible to attach a service account or use Workload Identity or Workload Identity Federation as appropriate authentication solutions. When you find yourself in these unique situations where other authentication methods cannot be used (and exclusively in these circumstances), you should create a service account key for the application. Because service account keys are critical to the security of your application and must be protected from unauthorized access, it is essential to store them securely, preferably in a key vault, and update or rotate them frequently.

You can learn more about the best way to authenticate service accounts on Google Cloud:

<https://cloud.google.com/blog/products/identity-security/how-to-authenticate-service-accounts-to-help-keep-applications-secure>.

**Note:** Deleting user-managed service account keys may break communication with the applications that are using the corresponding keys. Make sure that your key pairs are reviewed before removal.



When designing and evaluating your firewall rules, keep in mind the following best practices:

- Implement least-privilege principles. Block all traffic by default and only allow the specific traffic you need. This includes limiting the rule to just the protocols and ports you need.
- Use hierarchical firewall policy rules to block traffic that should never be allowed at an organization or folder level.
- For allow rules, restrict them to specific VMs by specifying the service account of the VMs.
- If you need to create rules based on IP addresses, try to minimize the number of rules. It's easier to track one rule that allows traffic to a range of 16 VMs than it is to track 16 separate rules.
- Turn on Firewall Rules Logging and use Firewall Insights to verify that firewall rules are being used in the intended way. Firewall Rules Logging can incur costs, so you might want to consider using it selectively.

## Logging Disabled

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location          | [REDACTED]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Risk              | Low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Required Skill    | High                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Affected Services | VPC, Cloud Tasks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Description       | <p>We have identified several services that have disabled logging. In case of security issues logs are very helpful to analyze such situations and for implementing the prevention of similar issues in the future. Following types of logs are not enabled:</p> <p><b>VPC Firewall rules</b></p> <p>The following VPC network firewall rules are not logged:</p> <p>VPC: [REDACTED]</p> <ul style="list-style-type: none"> <li>• [REDACTED]</li> </ul> <p>VPC: [REDACTED]</p> <ul style="list-style-type: none"> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> </ul> <p>Firewall rule logging allows you to verify, analyze, and audit the effects of your VPC firewall rules on your cloud resources. For example, you can determine if a firewall rule designed to deny network traffic is functioning as intended. This type of logging is also useful if you need to determine how many connections are affected by a given VPC firewall rule.</p> <p>Following command can be used to verify it:</p> <pre>[REDACTED]</pre> <p><b>VPC Flow logs - subnets</b></p> <p>VPC Flow logging is disabled for all subnets in the default VPC and for the following subnet in the [REDACTED] VPC:</p> <ul style="list-style-type: none"> <li>• [REDACTED]</li> </ul> <p>Following command can be used to verify it:</p> <pre>[REDACTED]</pre> |



By default, the VPC Flow Logs feature is disabled when a new VPC network subnet is created. Once enabled, VPC Flow Logs will start collecting network traffic data to and from your Virtual Private Cloud subnets, logging data that can be useful for understanding network usage, network traffic expense optimization, network forensics, and real-time security analysis. To enhance Google Cloud VPC network visibility and security it is strongly recommended to enable Flow Logs for every business-critical or production VPC subnet.

### Cloud Tasks

The following Cloud Tasks queue has audit logs disabled:

- 

Use Cloud Audit Logs to keep track of who did what, when, and where for your Cloud Tasks. This can help you understand how your task queues are being accessed and used, and can also support your compliance requirements.

### Mitigation

We recommend enabling logging in to all relevant GCP services. Logging data can be useful to detect and troubleshoot security issues within your GCP account/projects.

We also recommend enabling audit logs for Cloud Tasks queues, especially those that process sensitive, critical, or otherwise important data. Audit logs provide invaluable information about traffic and access to your services that can be crucial for troubleshooting, security investigations, and compliance.

Please note that while audit logs are important for maintaining the security and integrity of your data, they can also generate large volumes of data in the case of queues and could therefore increase your costs. Therefore, it is recommended that you tailor your audit logging strategy to balance both your security and cost-effectiveness needs. You can do this by selectively enabling audit logs only for queues that deal with sensitive or business-critical data.

## Default VPC Network In Use

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location           | ██████████                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Risk               | Informational                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Required Skill     | High                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Affected Services: | VPC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Description        | <p>We have identified that a default Virtual Private Cloud (VPC) is used. A default Virtual Private Cloud (VPC) is designed in such a way that you can quickly deploy GCP resources and not have to think about the underlying network. The default VPC comes with a predefined network configuration that automatically generates 4 over-permissive, insecure firewall rules, that are not included in the audit logging:</p> <ul style="list-style-type: none"> <li>• ██████████ – This rule allows ingress connections for all TCP, UDP and ICMP protocols and all ports (0-65535) among VM instances within the network.</li> <li>• ██████████ – Allows ingress connections on TCP port ████████ (SSH) from any source to any virtual machine (VM) instance in the network.</li> <li>• ██████████ – This firewall rule allows ingress connections on TCP port ████████ (RDP) from any source to any VM instance in the network.</li> <li>• ██████████ – Allows ingress ICMP traffic from any source to any VM instance within the network.</li> </ul> <p>The default Virtual Private Cloud (VPC) network is also an auto-mode network, which means that its subnets use the same predefined range of IPv4 addresses, and as a result, it's not possible to use Cloud VPN or VPC Network Peering feature with the default network. A default VPC might be suitable for getting started quickly with your GCP project, however, when you deploy complex, production applications and use multi-tier architectures, you may need to keep parts of your network private or customize the network model, therefore it is recommended to create a non-default VPC that suits your specific project requirements.</p> <p>Following command can be used to verify it:</p> <pre>gcloud compute networks list</pre> |
| Mitigation         | <p>In order to follow security best practices and meet networking requirements, we recommend that you remove the default Virtual Private Cloud (VPC) network from your GCP project and migrate your cloud applications to the ██████████ VPC. More information can be found at: <a href="https://cloud.google.com/vpc/docs/vpc#default-network">https://cloud.google.com/vpc/docs/vpc#default-network</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Cloud SQL

### Database Instances with Public IPs

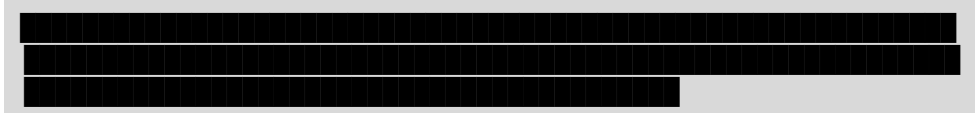
|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location           | [REDACTED]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Risk               | Low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Required Skill     | High                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Affected Services: | Cloud SQL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Description        | <p>We have found that the following Cloud SQL instances have a public IP address:</p> <p>Production:</p> <ul style="list-style-type: none"> <li>• [REDACTED]</li> <li>• [REDACTED]</li> </ul> <p>Development:</p> <ul style="list-style-type: none"> <li>• [REDACTED]</li> </ul> <p>Staging:</p> <ul style="list-style-type: none"> <li>• [REDACTED]</li> <li>• [REDACTED]</li> </ul> <p>The following command can be used to verify it:</p> <pre>[REDACTED]</pre> <p>This is understandable since you are using Cloud SQL Auth proxy to connect from the Internet. No external networks are authorized to connect to your Cloud SQL instance. However, a public IP address can increase your attack surface, even if no authorized networks are configured and you are using the SQL Auth proxy as a secure connection method.</p> <p>In a rapidly evolving Cloud services environment, configurations can be complex and it can be very easy to misconfigure. A single oversight can potentially expose sensitive resources to threats.</p> <p>To reduce the attack surface, Cloud SQL databases should only have private IPs attached. Private IPs provide better Cloud network security and lower latency for your database applications.</p> |
| Mitigation         | <p>To further enhance the security of your database, we recommend that you consider additional methods of securing your connection to Cloud SQL. If you need to access the DB instance for data-entry, troubleshooting, monitoring or maintenance, you can use one of the following approaches:</p> <ol style="list-style-type: none"> <li>1. <b>Use a VPN or Cloud Interconnect to establish a private connection to your GCP project:</b> If your usage patterns and infrastructure allow it, you might consider connecting to the SQL instance over a private IP address through a</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

- secure VPN tunnel or Cloud Interconnect. This option would require more configuration, but would completely eliminate the need for a public IP, reducing your exposure to the Internet.
2. **Establish a secure connection to the Cloud SQL database using a bastion host:** Another secure method is to use a bastion host (also known as a jump server), which acts as a gateway between the secure internal network and the external Internet. For this bastion host, you can set up strict security policies and firewall rules that allow only necessary traffic from known, trusted sources. From the bastion host, you can then securely connect to the Cloud SQL instance.
  3. **Cloud SQL Auth Proxy with Cloud IAP (Identity-Aware Proxy):** Using Google Cloud Identity-Aware Proxy (IAP), you can control access to your Cloud SQL instance at the application layer. This means that you can enforce access control policies based on a user's identity and the context of their request, providing an additional layer of security. More information can be found at [https://www.youtube.com/watch?v=rebyg9\\_eTHM](https://www.youtube.com/watch?v=rebyg9_eTHM).

## Encryption in Transit not Enforced

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location           | [REDACTED]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Risk               | Low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Required Skill     | High                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Affected Services: | Cloud SQL, Memorystore for Redis                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Description        | <p>Encryption in transit is an important security measure that helps protect data from interception, tampering or theft during transmission over the network. When data is sent over a network - whether between two applications, between a client and a server, or to and from a cloud provider - it can potentially be exposed to a variety of risks if it is not adequately secured.</p> <p>During our security audit, we identified instances where encryption in transit was not enabled for Cloud SQL and Memorystore for Redis.</p> <p><b>Cloud SQL</b></p> <p>The following Cloud SQL instances allow unencrypted connections:</p> <ul style="list-style-type: none"> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> </ul> <p>Following command can be used to verify it:</p> <pre>[REDACTED]</pre> <p>Setting up your Cloud SQL instance to accept SSL/TLS connections enables SSL/TLS connections for the instance, but unencrypted and unsecure connections are still accepted. If you do not require SSL/TLS for all connections, clients without a valid certificate are allowed to connect. For this reason, if you are accessing your instance using public IP, it is strongly recommended that you enforce SSL for all connections.</p> <p>When the requiring SSL/TLS option is enabled, you can use either the Cloud SQL Auth proxy or SSL/TLS certificates to connect to your Cloud SQL instance.</p> <p><b>Memorystore for Redis</b></p> <p>The following Redis instance is configured with disabled in-transit data encryption:</p> <ul style="list-style-type: none"> <li>• [REDACTED]</li> </ul> |

Following command can be used to verify it:



Memorystore for Redis includes the ability to encrypt all traffic using the Transport Layer Security (TLS) protocol, ensuring that data transmitted between the Redis client and server is secure. When this feature is enabled, clients must communicate exclusively over a secure port connection. Any clients that do not have TLS configured will not be able to establish a connection.

Unencrypted connections between the Redis client and the server expose your data to potential risks such as eavesdropping and unauthorized modification. Therefore, it is strongly recommended that you activate encryption in transit to protect your data as it traverses the network.

#### Mitigation

If in-transit encryption is disabled, this means that the data is sent in clear text and can be intercepted or tampered with during transmission. This can potentially lead to unauthorised access, data breaches and other security incidents. Enabling encryption in transit is therefore a recommended best practice to secure data in motion.

#### Cloud SQL

We recommend that you configure your Cloud SQL database instances to enforce SSL/TLS for all incoming connections. Using the Cloud SQL Auth proxy does not require SSL/TLS certificates because the connection is encrypted regardless of the setting.

#### Memorystore for Redis

The configuration of your Redis instance should include encryption of transmitted data. This measure greatly reduces the likelihood of any sensitive data being exposed during transmission. In addition, if you have the AUTH feature enabled, encryption in transit is highly recommended to ensure that your login credentials are kept confidential as they traverse the network.

However, it is important to note that enabling in-transit encryption on your Redis instance introduces limits on the **maximum number of client connections** your instance can have. The limit is dependent on your instance size.

#### Encryption in Transit by Default

According to Google's documentation, Google uses a variety of methods, both default and user-configurable, to encrypt transmitted data. The type of encryption used depends on the OSI layer, the type of service and the physical infrastructure component. We recommend reading the white paper on how Google uses encryption to protect your data, available at

<https://cloud.google.com/docs/security/encryption-in-transit>.

If you are confident that client traffic meets VPC network level based encryption on Google Cloud encryption standards

([https://cloud.google.com/docs/security/encryption-in-transit#encryption\\_in\\_transit\\_by\\_default](https://cloud.google.com/docs/security/encryption-in-transit#encryption_in_transit_by_default)), there is no need to implement additional in-transit encryption for these services.

## Log\_error\_verbosity Database Flag for Cloud SQL PostgreSQL Instance Is NOT Set to DEFAULT or Stricter

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location           | ████████████████████                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Risk               | Low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Required Skill     | High                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Affected Services: | Cloud SQL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Description        | <p>The following PostgreSQL Instances have not 'log_error_verbosity' flag set to 'default':</p> <ul style="list-style-type: none"><li>• Production: ██████████ and ██████████</li><li>• Development: ██████████</li><li>• Staging: ██████████ and ██████████</li></ul> <p>The log_error_verbosity flag controls the verbosity/details of messages logged. TERSE excludes the logging of DETAIL, HINT, QUERY, and CONTEXT error information. VERBOSE output includes the SQLSTATE error code, source code file name, function name, and line number that generated the error. Ensure an appropriate value is set to 'DEFAULT' or stricter.</p> |
| Mitigation         | <p>Auditing helps in troubleshooting operational problems and also permits forensic analysis. If log_error_verbosity is not set to the correct value, too many details or too few details may be logged. This flag should be configured with a value of 'DEFAULT' or stricter.</p> <p>References : <a href="https://cloud.google.com/sql/docs/postgres/flags">https://cloud.google.com/sql/docs/postgres/flags</a></p>                                                                                                                                                                                                                        |

## 'cloudsql.enable\_pgaudit' Database Flag for each Cloud Sql Postgresql Instance Is Set to 'on' For Centralized Logging

|                    |                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location           | [REDACTED]                                                                                                                                                                                                                                                                                                                                                                                                |
| Risk               | Low                                                                                                                                                                                                                                                                                                                                                                                                       |
| Required Skill     | High                                                                                                                                                                                                                                                                                                                                                                                                      |
| Affected Services: | Cloud SQL                                                                                                                                                                                                                                                                                                                                                                                                 |
| Description        | <p>The following PostgreSQL Instances have not 'cloudsql.enable_pgaudit' flag set to 'on'</p> <ul style="list-style-type: none"><li>• Production: [REDACTED] and [REDACTED]</li><li>• Development: [REDACTED]</li><li>• Staging: [REDACTED] and [REDACTED]</li></ul> <p>Ensure cloudsql.enable_pgaudit database flag for Cloud SQL PostgreSQL instance is set to on to allow for centralized logging.</p> |
| Mitigation         | <p>Enable pgAudit flag.</p> <p>References: <a href="https://cloud.google.com/sql/docs/postgres/flags">https://cloud.google.com/sql/docs/postgres/flags</a></p>                                                                                                                                                                                                                                            |

## Cloud SQL Database Instances are not Configured With Automated Backups

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location           | ████████████████████████████████████████                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Risk               | Low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Required Skill     | High                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Affected Services: | Cloud SQL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Description        | <p>The following database Instances do not have automated backups configured:</p> <ul style="list-style-type: none"><li>• ██████████ (████████████████)</li><li>• ██████████</li></ul> <p>Backups provide a way to restore a Cloud SQL instance to recover lost data or recover from a problem with that instance. Automated backups need to be set for any instance that contains data that should be protected from loss or damage. This recommendation is applicable for SQL Server, PostgreSQL, MySQL generation 1 and MySQL generation 2 instances.</p> |
| Mitigation         | <p>It is recommended to have all SQL database instances set to enable automated backups.</p> <p>References: <a href="https://cloud.google.com/sql/docs/postgres/configure-ssl-instance/">https://cloud.google.com/sql/docs/postgres/configure-ssl-instance/</a></p>                                                                                                                                                                                                                                                                                          |

## Missing logging Flags

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location           | [REDACTED]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Risk               | Informational                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Required Skill     | High                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Affected Services: | Cloud SQL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Description        | <p>The following database flags are not enabled for your Google Cloud SQL database instances:</p> <p><b>Flag:</b> <code>log_min_duration_statement</code></p> <p>The <code>log_min_duration_statement</code> configuration flag causes the duration of each completed SQL statement to be logged if the statement executes for at least the specified number of milliseconds. Setting this flag to 0 logs all statement durations, whereas setting it to -1 disables logging statement durations. Logging SQL statements may include sensitive information that should not be recorded in log files, therefore the <code>log_min_duration_statement</code> database flag should be disabled.</p> <p>Affected SQL instances:</p> <ul style="list-style-type: none"> <li>• [REDACTED]</li> <li>• [REDACTED]</li> </ul> <p>Following command can be used to verify it:</p> <pre>[REDACTED]</pre> <p><b>Flag:</b> <code>log_connections</code></p> <p>By default, the PostgreSQL database engine does not log attempted connections. Enabling the <code>log_connections</code> flag will create log entries for each attempted connection as well as entries for successful completion of client authentication. The logging data generated by this configuration flag can be used to identify, troubleshoot, and repair configuration errors and sub-optimal performance for your Google Cloud PostgreSQL database instances.</p> <p>Affected SQL instances:</p> <ul style="list-style-type: none"> <li>• [REDACTED]</li> <li>• [REDACTED]</li> </ul> <p>Following command can be used to verify it:</p> <pre>[REDACTED]</pre> |

```
[REDACTED]
```

**Flag:** `log_disconnections`

By default, `log_disconnections` configuration flag is disabled. PostgreSQL database engine does not log information such as session duration and session end by default. Enabling the `log_disconnections` flag starts recording PostgreSQL activity data that can be useful to identify, troubleshoot, and repair configuration errors and sub-optimal performance for your Cloud PostgreSQL database instances.

Affected SQL instances:

- [REDACTED]
- [REDACTED]

Following command can be used to verify it:

```
[REDACTED]
```

**Flag:** `log_lock_waits`

The "deadlock\_timeout" PostgreSQL configuration setting defines the time to wait on a lock before checking for any conditions. Frequent exceeding of the "deadlock\_timeout" value (time) can be an indication of underlying security and performance issues. Logging such waits on locks by enabling the `log_lock_waits` database flag can be used to identify poor performance due to locking delays. This can also be used to determine if an SQL statement is attempting to starve resources through holding locks for excessive amounts of time.

Affected SQL instances:

- [REDACTED]

Following command can be used to verify it:

```
[REDACTED]
```

**Flag:** `log_temp_files`

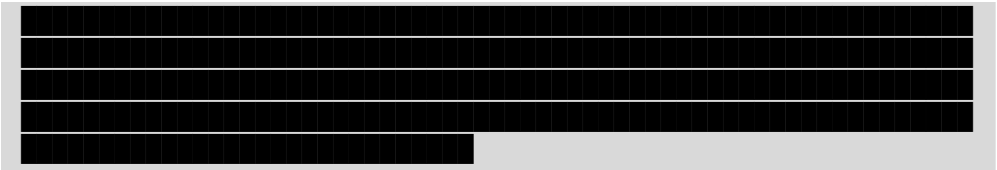
A value of -1 disables temporary file information logging. By default, the `log_temp_files` flag is set to -1 within the Google Cloud PostgreSQL instances configuration. When temporary files are not logged at all, it may be difficult to identify potential performance issues that can be created by poor programming practices or deliberate resource starvation attempts.

Affected SQL instances:

- [REDACTED]

Following command can be used to verify it:

```
[REDACTED]
```



Mitigation

We recommend enabling/disabling the database flags described above for your Cloud SQL database instances.

## Compute Engine

### Block Project-Wide SSH Keys feature disabled

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location           | [REDACTED]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Risk               | Low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Required Skill     | High                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Affected Services: | Compute Engine                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Description        | <p>The following VM instances are not configured to ignore GCP project-wide (shared) public SSH keys:</p> <p>Production:</p> <ul style="list-style-type: none"> <li>[REDACTED]</li> <li>[REDACTED]</li> <li>[REDACTED]</li> </ul> <p>Development:</p> <ul style="list-style-type: none"> <li>[REDACTED]</li> <li>[REDACTED]</li> <li>[REDACTED]</li> </ul> <p>Staging:</p> <ul style="list-style-type: none"> <li>[REDACTED]</li> </ul> <p>Project-wide SSH keys can be used to log in to all the Google Cloud VM instances running inside a GCP project. The project-wide SSH keys can ease the SSH key management but if compromised, they pose a security risk which can impact all the VM instances within the project, therefore it is strongly recommended to use instance-specific SSH keys as these keys can limit the attack surface if they are compromised. By default, the <code>Block Project-Wide SSH Keys</code> security feature is not enabled for Google Compute Engine instances.</p> |
| Mitigation         | We recommend enabling the <code>Block Project-Wide SSH Keys</code> security feature and block users with common/shared project-wide SSH keys from connecting to your Google Cloud VM instances.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## OS Patch Management not configured

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location           | [REDACTED]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Risk               | Low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Required Skill     | High                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Affected Services: | Compute Engine                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Description        | <p>OS Patch Management is not configured for the following VM instances:</p> <ul style="list-style-type: none"> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> </ul> <p style="text-align: center;">-IMAGE REDACTED-<br/>Image OS patch management disabled</p> <p>This leaves your VMs potentially vulnerable to known operating system security issues that could be mitigated through patching.</p> <p>Operating system patches often contain security enhancements that protect your system from known vulnerabilities, malware, and other threats. By not having a patch management process in place, your organization may be exposing itself to unnecessary risks.</p> <p>In addition, this lack of patch management could be in violation of many security standards and regulations, which often require regular patching and updates to systems to ensure a secure environment.</p> |
| Mitigation         | <p>Use OS patch management to apply operating system patches across a set of Compute Engine VM instances (VMs). Long running VMs require periodic system updates to protect against defects and vulnerabilities. More information can be found at <a href="https://cloud.google.com/compute/docs/os-patch-management">https://cloud.google.com/compute/docs/os-patch-management</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## 'Enable Connecting to Serial Ports' Is enabled for VM Instance

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location           | ████████████████████████████████████████                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Risk               | Low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Required Skill     | High                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Affected Services: | Compute Engine                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Description        | <p>VM Instance ████████████████████████████████████████ have 'Enable Connecting to Serial Ports' set to on</p> <p>If you enable the interactive serial console on your VM instance, clients can attempt to connect to your instance from any IP address and this allows anybody to access the instance if they know the user name, the SSH key, the project ID, and the instance name and zone.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Mitigation         | <p>Ensure that "Enable connecting to serial ports" configuration setting is disabled for all your production Google Compute Engine instances. A Google Cloud virtual machine (VM) instance has 4 virtual serial ports. On your VM instances, the operating system (OS), BIOS, and other system-level entities write often output data to the serial ports and can accept input, such as commands or answers, to prompts. Usually, these system-level entities use the first serial port (Port 1) and Serial Port 1 is often referred to as the interactive serial console. This interactive serial console does not support IP-based access restrictions such as IP address whitelists. To adhere to cloud security best practices and reduce the risk of unauthorized access, interactive serial console support should be disabled for all instances used in production.</p> <p>References: <a href="https://cloud.google.com/compute">https://cloud.google.com/compute</a></p> |

## OS Login for GCP Projects disabled

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location           | [REDACTED]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Risk               | Informational                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Required Skill     | High                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Affected Services: | Compute Engine, Project                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Description        | <p>We have identified that the GCP project [REDACTED] does not have OS Login feature enabled. Enabling OS Login feature ensures that the SSH keys used to connect to VM instances are mapped with Google Cloud IAM users. Revoking access to corresponding IAM users will revoke all the SSH keys associated with these users, therefore it facilitates centralized SSH key pair management, which is extremely useful in handling compromised or stolen SSH key pairs and/or revocation of external/third-party/vendor users.</p> <p>Following command can be used to verify it:</p> <pre>[REDACTED]</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Mitigation         | <p>We recommend that you enable the OS Login feature at the Google Cloud Platform (GCP) project level. More information can be found at <a href="https://cloud.google.com/compute/docs/oslogin">https://cloud.google.com/compute/docs/oslogin</a>.</p> <p>For all business-critical VM instances, we recommend that you configure OS Login with 2FA Authentication. When Two-Factor Authentication (2FA) is configured with OS Login, the user (e.g. instance administrator) will have to present a minimum of two separate forms of authorization before its access is granted. Having an MFA-protected instance represents an efficient way to safeguard your production and business-critical applications against malicious actors, as attackers would have to compromise at least two different authentication methods in order to gain access to your VM instance, and this reduces significantly the risk of attack.</p> <p><b>Important note:</b> Enabling OS Login for a GCP project disables metadata-based SSH key configurations on all the Google Compute Engine instances available within that project.</p> |

## Logging

### NO Log Metric Filter and Alerts

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location           | ████████████████████                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Risk               | Medium                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Required Skill     | High                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Affected Services: | logging                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Description        | <ul style="list-style-type: none"> <li> <b>Project Ownership Assignments/Changes</b><br/> There are no log metric filters or alerts associated with project ██████████. Project ownership has the highest level of privileges on a GCP project. These privileges include viewer permissions on all GCP services inside the project, permission to modify the state of all GCP services within the project, set up billing and manage roles and permissions for the project and all the resources inside the project. </li> <li> <b>Audit Configuration Changes</b><br/> There are no log metric filters or alerts associated with project ██████████. Admin Activity audit logs and Data Access audit logs produced by the Google Cloud Audit Logs service can be extremely useful for security analysis, resource change tracking, and compliance auditing. </li> <li> <b>Cloud Storage IAM Permission Changes</b><br/> There are no log metric filters or alerts associated with project ██████████. Monitoring changes to cloud storage bucket permissions may reduce the time needed to detect and correct permissions on sensitive cloud storage buckets and objects inside the bucket. </li> <li> <b>Custom Role Changes</b><br/> There are no log metric filters or alerts associated with project ██████████. Google Cloud IAM provides predefined roles that give granular access to specific Google Cloud Platform resources and prevent unwanted access to other resources. </li> <li> <b>SQL Instance Configuration Changes</b><br/> There are no log metric filters or alerts associated with project ██████████. Monitoring changes to SQL instance configuration changes may reduce the time needed to detect and correct misconfigurations done on the SQL server. </li> <li> <b>VPC Network Changes</b><br/> There are no log metric filters or alerts associated with project ██████████. Monitoring changes to a VPC will help ensure VPC traffic flow is not getting impacted </li> <li> <b>VPC Network Firewall Rule Changes</b><br/> There are no log metric filters or alerts associated with project ██████████. Monitoring for Create or Update Firewall rule events gives insight to network access changes and may reduce the time it takes to detect suspicious activity. </li> </ul> |

- **VPC Network Route Changes**

There are no log metric filters or alerts associated with project [REDACTED]. Monitoring changes to route tables will help ensure that all VPC traffic flows through an expected path.

Mitigation

- Ensure Log Metric Filter and Alerts Exist for Project Ownership Assignments/Changes. Using Google Cloud alerting policies to detect ownership assignments/changes will help you maintain the right access permissions for each IAM member created within your project, follow the security principle of least privilege, and prevent any accidental or intentional changes that may lead to unauthorized actions.
- By using Google Cloud alerting policies to detect audit configuration changes, you make sure that the recommended state of audit configuration is well maintained so that all the activities performed within your GCP project are available for security analysis and auditing at any point in time.
- Ensure That the Log Metric Filter and Alerts Exist for Cloud Storage IAM Permission Changes. It is recommended that a metric filter and alarm be established for Cloud Storage Bucket IAM changes.
- Ensure That the Log Metric Filter and Alerts Exist for Custom Role Changes. It is recommended that a metric filter and alarm be established for changes to Identity and Access Management (IAM) role creation, deletion and updating activities.
- Ensure That the Log Metric Filter and Alerts Exist for SQL Instance Configuration Changes. It is recommended that a metric filter and alarm be established for SQL instance configuration changes.
- Ensure That the Log Metric Filter and Alerts Exist for VPC Network Changes. It is recommended that a metric filter and alarm be established for Virtual Private Cloud (VPC) network changes.
- Ensure That the Log Metric Filter and Alerts Exist for VPC Network Firewall Rule Changes. It is recommended that a metric filter and alarm be established for Virtual Private Cloud (VPC) Network Firewall rule changes.
- Ensure That the Log Metric Filter and Alerts Exist for VPC Network Route Changes. It is recommended that a metric filter and alarm be established for Virtual Private Cloud (VPC) network route changes.

References: <https://cloud.google.com/monitoring/alerts>

## NO least one sink used to export copies of all the log entries

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location           | ████████████████████████████████████████                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Risk               | Low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Required Skill     | High                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Affected Services: | logging                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Description        | <ul style="list-style-type: none"><li>• Sink_Required is enabled but not exporting copies of all the log entries in projects ██████████ and ██████████ and ██████████</li><li>• Sink_Default is enabled but not exporting copies of all the log entries in projects ██████████ and ██████████ and ██████████</li></ul> <p>If sinks are not created, logs would be deleted after the configured retention period, and would not be backed up.</p>                                        |
| Mitigation         | <p>Ensure there is at least one sink used to export copies of all the log entries.</p> <p>It is recommended to create a sink that will export copies of all the log entries. This can help aggregate logs from multiple projects and export them to a Security Information and Event Management (SIEM).</p> <p>References</p> <ul style="list-style-type: none"><li>• <a href="https://cloud.google.com/logging/docs/export">https://cloud.google.com/logging/docs/export</a></li></ul> |



### App Engine

The following App Engine application is currently configured to accept traffic from all network origins:

- [REDACTED]

The following command can be used to verify it:

```
[REDACTED]
```

This is the default behavior of App Engine applications when they are first deployed. At the time of our assessment, no services or instances were currently running in this App Engine environment.

Although this is the default setting, it is not considered a best practice in terms of security. Accepting traffic from all network sources can unnecessarily expose your application to potential threats. Even if no services or instances are currently running, having such an open policy increases your potential attack surface once services or instances are running. This could lead to an increased number of unauthorized access attempts, data leakage, or resource misuse.

### Cost Implications

In addition to the security risks, it is important to note that publicly accessible services may also attract more bot traffic or malicious requests, which can lead to higher usage and, consequently, higher costs. Furthermore, if these services are involved in a security incident, the subsequent investigation and recovery efforts can also lead to additional costs.

### Mitigation

Most GCP services described in this chapter are probably intentionally available from the internet. However, we recommend to consider the following measures:

#### Cloud Run

To have a stronger guarantee that no malicious requests can reach your backend instances, prevent the Cloud Run instances from receiving inbound traffic initiated by someone on the Internet by configuring the ingress settings to Internal or Internal and Cloud Load Balancing. If you require remote connectivity with your private Cloud Run services over the public internet, we recommend using GCP API Gateway service, Cloud Endpoints or Cloud Load Balancing, as these services provide additional security features such as DDoS protection, WAF integration (in case of Load Balancer), authentication/authorization, rate limiting, etc.

By restricting the ingress settings, you can ensure that even if authentication credentials are compromised or a vulnerability in the authentication process occurs, access to Cloud Run will be restricted to trusted sources. This can significantly improve the overall security of Cloud Run and help mitigate potential risks.

More information can be found here:

- <https://cloud.google.com/endpoints/docs/openapi/set-up-cloud-run-esp-v2>
- <https://cloud.google.com/api-gateway/docs/get-started-cloud-run>
- <https://cloud.google.com/run/docs/securing/ingress>
- <https://cloud.google.com/load-balancing/docs/https/setup-global-ext-https-serverless>
- <https://servian.dev/external-ingress-control-for-cloud-run-afb3852c0d57>

### App Engine

We recommend adopting a more restrictive network policy and applying the principle of least privilege. This principle means that a service or application should only be exposed to the minimum necessary set of network origins.

You can use App Engine firewall rules to implement this policy. These allow you to control access to the App Engine application by allowing you to specify a range of IP addresses that are allowed or denied access. In a typical scenario, you might want to allow only traffic from certain IP ranges (for example, from the corporate network, VPN, or other GCP services) and disallow all other traffic.

You can also restrict inbound traffic to the App Engine using the Ingress controls. Ingress is set at the service level.

Remember that even if no services or instances are currently running, it is critical to keep security in mind for future deployments. Therefore, by modifying your network policy now, you can better prepare your App Engine environment for secure use in the future.

Relevant resources:

- [https://cloud.google.com/appengine/docs/flexible/application-security?tab=python#app\\_engine\\_firewall](https://cloud.google.com/appengine/docs/flexible/application-security?tab=python#app_engine_firewall)
- [https://cloud.google.com/appengine/docs/flexible/application-security?tab=python#ingress\\_controls](https://cloud.google.com/appengine/docs/flexible/application-security?tab=python#ingress_controls)

## Uniform Bucket-Level Access for Cloud Storage Buckets

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location           | [REDACTED]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Risk               | Low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Required Skill     | High                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Affected Services: | Cloud Storage                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Description        | <p>Following Google Cloud Storage buckets have uniform bucket-level access feature disabled:</p> <p>Production:</p> <ul style="list-style-type: none"> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> </ul> <p>Development:</p> <ul style="list-style-type: none"> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> </ul> <p>Staging:</p> <ul style="list-style-type: none"> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> </ul> <p>Following command can be used to verify it:</p> <pre>[REDACTED]</pre> <p>Google Cloud Storage provides two systems for granting users permission to access your storage buckets and objects: Identity and Access Management (IAM) and Access Control Lists (ACLs). These systems can function in parallel, and for a user to access a Cloud Storage resource, only one of the systems needs to grant the user permission.</p> <p>IAM is used throughout Google Cloud Platform (GCP) and allows you to grant a variety of permissions at the project and bucket level (uniform). ACLs are used only by Cloud Storage and have limited permission options, but they allow you to grant permissions on a per-object basis (fine-grained).</p> |

Enabling uniform bucket-level access feature disables ACLs for all Cloud Storage resources (buckets and objects) so that the access is granted exclusively through IAM. The feature is also used to unify and simplify how you grant access to your Cloud Storage resources. By default, Google Cloud Storage buckets do not have the uniform bucket-level access feature enabled.

According to Google documentation, using uniform bucket-level access is recommended, because it unifies and simplifies how you grant access to your Cloud Storage resources. Using uniform bucket-level access also enables you to use other Google Cloud security features such as domain restricted sharing, workforce identity federation, and IAM Conditions.

#### Mitigation

To follow security best practices and ensure privacy and security of your data in Cloud Storage, enable uniform bucket-level access feature for all buckets in your GCP project, if possible. More information can be found at:

<https://cloud.google.com/storage/docs/uniform-bucket-level-access#should-you-use>.

**Note:** If you enable uniform bucket-level access, you revoke access from users who get their access exclusively through object ACLs. Certain Google Cloud Platform services, such as Cloud Audit Logs and Datastore, cannot export to Cloud Storage buckets that have uniform bucket-level access enabled.

## Key Rotation Disabled

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location           | [REDACTED]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Risk               | Low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Required Skill     | High                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Affected Services: | Secret Manager                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Description        | <p>Secrets stored in Secret Manager in GCP are not being rotated automatically (there are secrets older than 300 days), which poses a potential security risk as secrets that have been compromised or are no longer needed may remain active. This could allow unauthorized access to sensitive information or resources. It is recommended that automatic rotation of secrets be implemented in Secret Manager in GCP to ensure that secrets are regularly updated and that any compromised or unnecessary secrets are promptly removed. This can be achieved by using the built-in rotation feature in Secret Manager that allows you to set a schedule for automatically rotating the secrets.</p> <p>Following commands can be used to get a list of secrets and the number of days since they were created (latest version):</p> <p>OSX compatible command:</p> <pre>[REDACTED]</pre> <p>Linux compatible command:</p> <pre>[REDACTED]</pre> |
| Mitigation         | <p>While it's ideal to follow a regular rotation schedule for secrets stored in Google Cloud Secret Manager, we understand that not all secrets, such as API keys provided by third parties, can be changed through this process.</p> <p>In cases where you have control over the lifecycle of a secret, we strongly recommend enabling the automatic rotation feature provided by Secret Manager. This feature allows you to set up a rotation schedule, ensuring that secrets are updated regularly and minimizing the potential damage caused by a leaked secret.</p>                                                                                                                                                                                                                                                                                                                                                                           |

For secrets that cannot be rotated regularly, such as the third-party API keys mentioned above, consider implementing additional security controls. These may include monitoring for unusual activity, limiting the scope of each secret (e.g. credentials for database access) to the minimum required permissions, or isolate secrets from the applications that use them.

Balancing these measures will help maintain the integrity of your secrets while adapting to the restrictions that third-party services may impose.

## GCP Memorystore for Redis has AUTH disabled

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Risk               | Low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Required Skill     | High                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Affected Services: | Redis                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Description        | <p>We have found that the following Redis instance has AUTH feature disabled:</p> <ul style="list-style-type: none"> <li></li> </ul> <p style="text-align: center;">-IMAGE REDACTED-<br/>Image Memorystore for Redis - AUTH feature disabled</p> <p>AUTH is an optional security feature on Memorystore for Redis that requires incoming connections to authenticate with an AUTH string. Every AUTH string is a Universally Unique Identifier (UUID), and each Redis instance with AUTH enabled has a unique AUTH string.</p> <p>If you enable the AUTH feature on your Memorystore instance, incoming client connections must authenticate in order to connect. Existing connections that had not previously authenticated need to properly authenticate before they can continue issuing commands. Once a client authenticates with an AUTH string, it remains authenticated for the lifetime of that connection, even if you change the AUTH string.</p> <p>AUTH helps you ensure that known entities in your organization do not unintentionally access and modify your Redis instance.</p> |
| Mitigation         | <p>We recommend that you enable AUTH on your Memorystore for Redis instance to protect against unwanted or non-approved connections. However, AUTH does not provide security during data transportation.</p> <p>If in-transit encryption is not enabled, there is no guarantee that the command is encrypted in-transit end to end. This is because there is no guarantee that the client traffic is meeting the VPC network level based encryption on Google Cloud encryption standards (<a href="https://cloud.google.com/docs/security/encryption-in-transit#virtual-network">https://cloud.google.com/docs/security/encryption-in-transit#virtual-network</a>).</p> <p>More information can be found at <a href="https://cloud.google.com/memorystore/docs/redis/about-redis-auth">https://cloud.google.com/memorystore/docs/redis/about-redis-auth</a>.</p>                                                                                                                                                                                                                                                                                                                  |

## Encryption with Customer-Managed Keys

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location           | [REDACTED]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Risk               | Informational                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Required Skill     | High                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Affected Services: | Cloud SQL, Cloud Storage, Cloud Run, Secret Manager, Artifactory Registry, Pub/Sub, Redis, Compute Engine                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Description        | <p>During the security assessment, it was discovered that the following services are encrypted with Google-managed encryption keys instead of Customer-Managed Keys (CMKs).</p> <p><b>Cloud SQL</b></p> <p>All Cloud SQL database instances are encrypted with Google-managed encryption keys. Following command can be used to verify it:</p> <pre>[REDACTED]</pre> <p><b>Cloud Run</b></p> <p>All Cloud Run services are encrypted with Google-managed encryption keys. You can protect container images deployed to Cloud Run services using Cloud KMS customer managed encryption keys (CMEK).</p> <p><b>Cloud Storage</b></p> <p>All Cloud Storage buckets are encrypted at rest with Google-managed encryption keys. Following command can be used to verify it:</p> <pre>[REDACTED]</pre> <p><b>Secret Manager</b></p> <p>All Secret Manager secrets are encrypted at rest with Google-managed encryption keys.</p> <p><b>Artifact Registry</b></p> |

The `gcf-artifacts` repository is encrypted at rest with Google-managed encryption keys. Following command can be used to verify it:

```
gcloud artifacts repositories list --format="table[NAME,KEY]"
```

### Pub/Sub

All Pub/Sub topics are encrypted at rest with Google-managed encryption keys. Following command can be used to verify it:

```
gcloud pubsub topics list --format="table[NAME,KEY]"
```

### Redis

Redis instance [REDACTED] is encrypted at rest with Google-managed encryption keys.

-IMAGE REDACTED-  
Image Memorystore for Redis - CMEK disabled

### Compute Engine

All VM disks are encrypted with Google-managed encryption keys.

Production:

- The VM Instance [REDACTED] have the following unencrypted disks: [REDACTED].
- The VM Instance [REDACTED] has the following unencrypted disks: [REDACTED].
- The VM Instance [REDACTED] has the following unencrypted disks: [REDACTED].

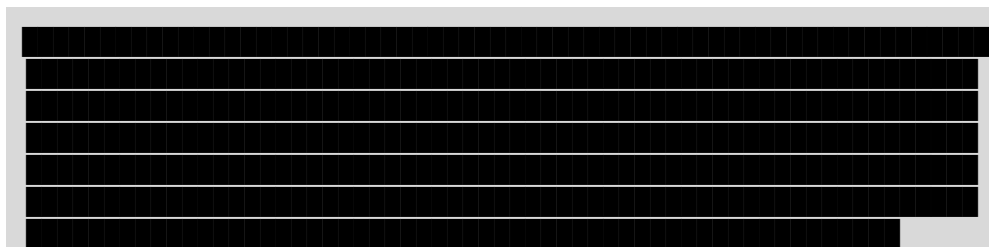
Development:

- The VM Instance [REDACTED] have the following unencrypted disks: [REDACTED].
- The VM Instance [REDACTED] have the following unencrypted disks: [REDACTED].
- The VM Instance [REDACTED] have the following unencrypted disks: [REDACTED].

Staging:

- The VM Instance [REDACTED] have the following unencrypted disks: [REDACTED].

Following command can be used to verify it:



This finding does not represent an issue or vulnerability. By default, Google Cloud services listed above encrypt all data using Google-managed encryption keys. The cloud service manages this type of encryption without any additional actions from you and your application. However, if you want to fully control and manage data encryption yourself, you can use your own Customer-Managed Keys (CMKs). Cloud KMS Customer-Managed Keys can be implemented to encrypt production, sensitive or business-critical data, and are often used in the enterprise world, where compliance and security controls are more stringent.

#### Mitigation

Using encryption at rest is an important part of data security. It provides a strong defensive barrier against unauthorised access and potential data breaches. In particular, when working with sensitive, business-critical data or adhering to compliance and security controls, the use of Google Cloud KMS Customer Managed Keys (CMK) should be prioritized.

Cloud KMS CMKs give you more control over the lifecycle, management and control of the cryptographic keys used to encrypt your data. With CMKs, you retain control over the generation, distribution, rotation, and retirement of encryption keys.

It's not just about protecting your data, it's about maintaining control and visibility over who can access it and when. By implementing CMK into your encryption strategy, you further strengthen your security posture and ensure compliance with regulatory requirements.

## Google Cloud API Keys in use

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Risk               | Informational                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Required Skill     | High                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Affected Services: | APIs & Services                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Description        | <p>We have identified that there is an API key called <code>Browser key</code>.</p> <p style="text-align: center;">-IMAGE REDACTED-<br/>Image Unrestricted Google Cloud API key</p> <p>Google Cloud Platform (GCP) API keys are simple encrypted strings that can be used when calling certain APIs which don't need to access private user data. GCP API keys are usually accessible to clients, as they can be publicly viewed from within a browser, making it easy to discover and steal an API key.</p> <p>The API key described above is also unrestricted. It can be considered insecure because it can be used by anyone, from anywhere. For production applications, you should set both application restrictions and API restrictions.</p> <p>Because only a limited number of Google Cloud services allow access using just API keys, without requiring another type of credential, Google recommends using a standard authentication flow instead of API keys for most applications. Deleting GCP API keys should enforce the use of secure authentication methods only and minimize exposure to attacks.</p> |
| Mitigation         | <p>When you use API keys in your applications, ensure that they are kept secure during both storage and transmission. Publicly exposing your API keys can lead to unexpected charges on your account. We also recommend deleting unused API keys.</p> <p>To help keep your API keys secure, follow the security best practices described here: <a href="https://cloud.google.com/docs/authentication/api-keys#securing">https://cloud.google.com/docs/authentication/api-keys#securing</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Artifact Registry - Vulnerability Scanning not Configured

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location           | ████████████████████████████████████████                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Risk               | Informational                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Required Skill     | High                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Affected Services: | Artifact Registry                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Description        | <p>Vulnerability scanning is disabled for Artifact Registry in GCP, which may allow for the presence of known vulnerabilities in container images stored within the registry. This poses a potential security risk as these vulnerabilities could be exploited by attackers. Vulnerability scanning automatically scans images when they are pushed to the registry for known security vulnerabilities and exposures.</p> <p>-IMAGE REDACTED-<br/>Image Container Registry - vulnerability scanning disabled</p> |
| Mitigation         | <p>It is recommended to enable vulnerability scanning for the Artifact Registry in the GCP to identify and mitigate any known vulnerabilities in the container images. However, at the time of writing the report, there were no docker images stored in the gcf-artifacts repository, so it does not make sense to enable this feature. If you plan to store container images in Artifact Registry in the future, we recommend enabling vulnerability scanning.</p>                                             |

# Appendix A: Security Evaluation Fixes

Will be updated by the Sayfer team after the first revision.