January 21, 2026

Security Posture Assessment

SPA - ANONYMIZED



Who are we... Zazmic Security Team

Zazmic is a Premier Google Cloud Partner dedicated to uncovering risks and establishing clear guides for remediation. At Zazmic, our Security Team brings together experienced engineers who are driven by results and committed to solving problems securely, not just finding them

What services we are offering:

- Vulnerability Assessment and Penetration Testing - Black box, Grey Box
- SPA - Security Posture Assessment of the GCP environment
- Google Workspace Security Audit
- CICD Security
- Support SOC2, Fedramp, ISO 27001, ISO 9001, HIPAA, HITRUST
- Google SecOps and Google SCCE licensing and setup

Contact Us:

Email: **sales@zazmic.com**
Join our security platform: **https://security.zazmic.com**

What is SPA?

Security Posture Assessment by Zazmic.

The Zazmic SPA tool is built by security engineers to uncover Google Cloud Security misconfigurations and make security understandable for everyone. Our reports are action-oriented and tailored to each customer, with remediation guidance shaped by experienced engineers.

What We Assess.

A deep evaluation across 5 critical security domains:

- Data Security
- Network Architecture
- Access & Permissions
- Backups & Secrets Management
- Monitoring & Threat Detection

How It Works.

- Kickoff & Scope Alignment
- 1-Week Deep-Dive Analysis
- Executive Report & Findings Review

What You Get.

- Detailed and Actionable Security Posture Assessment Report — clear visibility into cloud risks + a prioritized remediation roadmap.
- Live Demos of Google's Security Stack — SecOps & SCC in action to show optimal protection.

Why Zazmic?

By combining expert security assessment with scalable managed services, Zazmic helps your organization stay ahead of modern cyber threats—not just react to them.

Table of Contents

1 Document Control **5**

1.1 Team 5

1.2 List of Changes 5

1.3 Assessment Details 5

2 Executive Summary **6**

2.1 Vulnerability Distribution 6

2.2 Master Findings Table 7

3 Detailed Findings **8**

H-1: Instance Public Access Disabled 8

H-2: Open RDP 9

H-3: Open SSH 10

H-4: Service Account Admin 11

M-1: Database SSL Enabled 12

M-2: IP Forwarding Disabled 13

L-1: VM Instance Deletion Protection 14

L-2: Instance Default Service Account 15

A Appendix **16**

1 Document Control

1.1 Team

Contact	Details	Role
Bradley Clunie	E-Mail: bradley.clunie@zazmic.com	Pentester

1.2 List of Changes

Version	Description	Date
1.0	Initial report generation	Jan 21, 2026

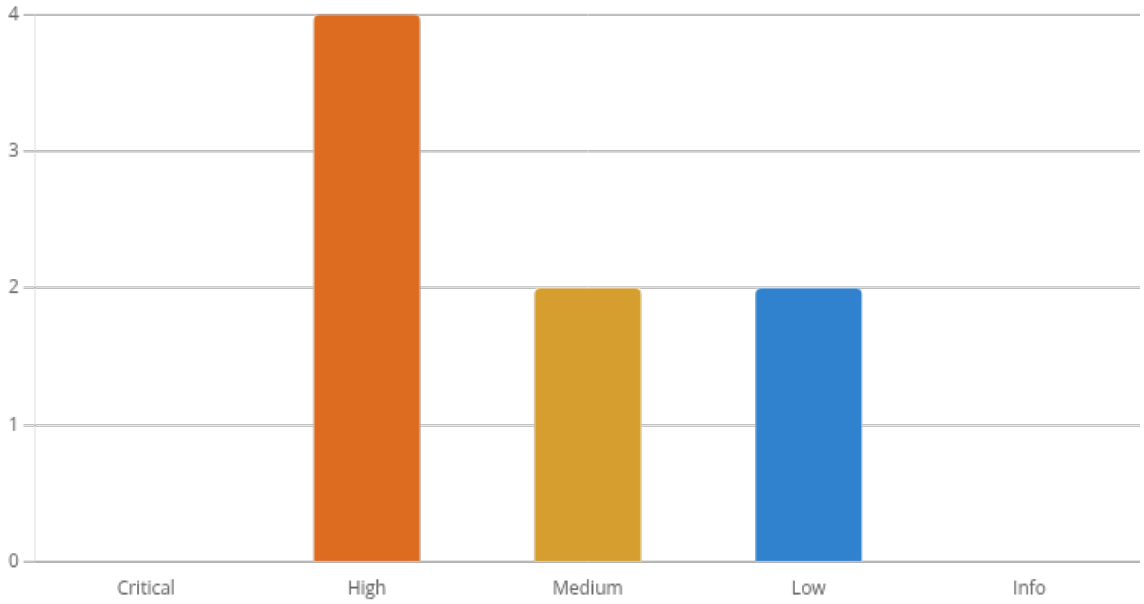
1.3 Assessment Details

Conduct Dates	January 21, 2026 to January 26, 2026
GCP Projects Scanned	• project-id

2 Executive Summary

This security assessment was conducted on Google Cloud Platform (GCP) resources using multiple tools and CLI commands to evaluate misconfigurations, vulnerabilities, and compliance adherence. The findings provide an in-depth look into security gaps affecting the GCP environment.

2.1 Vulnerability Distribution



High	Medium	Low
4	2	2

Calculated Score: 46/100 — Security Grade: D

Significant risk; multiple High/Critical vulnerabilities detected.

In the course of this security posture assessment **4 High**, **2 Medium** and **2 Low** findings were identified:

- **High-severity findings** represent significant misconfigurations that could lead to data exposure, unauthorized access, or compliance violations.
- **Medium-severity findings** indicate weaknesses that should be addressed to strengthen the overall security posture.
- **Low-severity findings** represent minor configuration gaps that should be remediated as part of ongoing security hygiene.

2.2 Master Findings Table

ID	Title	State	Severity
H-1	Instance Public Access Disabled	Fixed	~~High~~
H-2	Open RDP	Open	High
H-3	Open SSH	Fixed	~~High~~
H-4	Service Account Admin	Open	High
M-1	Database SSL Enabled	Fixed	~~Medium~~
M-2	IP Forwarding Disabled	Open	Medium
L-1	VM Instance Deletion Protection	Open	Low
L-2	Instance Default Service Account	Open	Low

3 Detailed Findings

H-1: Instance Public Access Disabled

~~High~~ Resolved

Identified on: April 6, 2026 | Resolved on: April 4, 2026

Affected Components: projects/project-id/zones/us-east5-b/instances/instance-id

References: https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address, https://cloud.google.com/security/best-practices/network-security, https://cloud.google.com/compute/docs/security/overview

Google Security Product: SecOps

Description

Ensures that compute instances are not configured to allow public access.

Public access is enabled for the instance

Recommendation

Disable public access for the instance by removing its external IP address. If public access is strictly necessary, ensure it is tightly controlled via firewall rules, and consider implementing a bastion host or VPN for secure access to minimize the attack surface.

H-2: Open RDP

High

Affected Components: projects/project-id/global/firewalls/firewall-rule

References: https://cloud.google.com/vpc/docs/firewalls, https://cloud.google.com/compute/docs/instances/connecting-to-windows#rdp, https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-073a

Google Security Product: SecOps

Description

Determines if TCP port 3389 for RDP is open to the public

Firewall Rule:firewall-rule) has RDP: TCP port 3389 open to 0.0.0.0/0

Recommendation

Restrict RDP access (TCP port 3389) to only trusted IP addresses or IP ranges. Consider using a bastion host, VPN, or Identity-Aware Proxy (IAP) for secure remote access instead of direct public RDP exposure. Ensure that any necessary RDP access is protected with strong authentication and regularly monitored.

H-3: Open SSH

~~High~~ Resolved

Identified on: March 18, 2026 | Resolved on: March 22, 2026

Affected Components: projects/project-id/global/firewalls/firewall-rule

References: https://cloud.google.com/vpc/docs/firewalls, https://cloud.google.com/compute/docs/instances/connecting-advanced#ssh_security_best_practices, https://www.ssh.com/academy/ssh/hardening

Google Security Product: SecOps

Description

Determines if TCP port 22 for SSH is open to the public

Firewall Rule:firewall-rule has SSH: TCP port 22 open to 0.0.0.0/0

Recommendation

Restrict SSH access (TCP port 22) to specific, trusted IP addresses or use Identity-Aware Proxy (IAP) for secure access, rather than allowing access from 0.0.0.0/0. Disable SSH access if not required for public internet access.

H-4: Service Account Admin

High

Affected Components: projects/project-id/serviceAccounts/sa@project-id.iam.gserviceaccount.com

References: https://cloud.google.com/iam/docs/best-practices, https://cloud.google.com/iam/docs/understanding-roles, https://cloud.google.com/run/docs/securing/iam

Google Security Product: SecOps

Description

Ensures that user managed service accounts do not have any admin, owner, or write privileges.

The Service account has the following permissions: roles/run.admin

Recommendation

Review the permissions granted to the service account 'projects/project-id/serviceAccounts/sa@project-id.iam.gserviceaccount.com'. Apply the principle of least privilege by replacing the 'roles/run.admin' role with more granular roles that provide only the necessary permissions for the service account's function. For example, if the service account only needs to invoke Cloud Run services, consider 'roles/run.invoker'. If it needs to deploy services, consider 'roles/run.developer' or a custom role with specific deployment permissions. Regularly audit service account permissions to ensure they remain appropriate.

M-1: Database SSL Enabled

~~Medium~~ Resolved

Identified on: April 1, 2026 | Resolved on: April 3, 2026

Affected Components: projects/project-id/instances/intance-id

References: https://cloud.google.com/sql/docs/postgres/configure-ssl, https://owasp.org/www-project-top-10/2017/A3_2017-Sensitive_Data_Exposure

Google Security Product: SecOps

Description

Ensures SQL databases have SSL enabled

SQL database has SSL disabled

Recommendation

Enable SSL/TLS for the SQL database instance 'database-id' to encrypt data in transit between the database and its clients. Ensure that client applications are configured to enforce SSL connections. Regularly review and update SSL/TLS configurations to use strong ciphers and protocols.

M-2: IP Forwarding Disabled

Medium

Affected Components: projects/project-id/zones/us-east5-b/instances/instance-id

References: https://cloud.google.com/compute/docs/instances/create-instance-with-custom-network-configuration, https://cloud.google.com/vpc/docs/firewalls, https://www.cisecurity.org/benchmark/google_cloud

Google Security Product: SecOps

Description

Ensures that IP forwarding is disabled on all instances

Instance has IP forwarding enabled

Recommendation

Review the necessity of IP forwarding on the instance 'instance-id'. If IP forwarding is not required for the instance's intended function, it should be disabled to reduce the attack surface. If it is required (e.g., for a VPN gateway), ensure that the instance is hardened, its network access is strictly controlled via firewall rules, and it is continuously monitored for suspicious activity. For Linux instances, IP forwarding can typically be disabled by setting 'net.ipv4.ip_forward = 0' in /etc/sysctl.conf and applying with 'sysctl -p'.





L-1: VM Instance Deletion Protection

Low

Affected Components: projects/project-id/zones/us-east5-b/instances/instance-id

References: https://cloud.google.com/compute/docs/instances/prevent-deleting-instance

Google Security Product: SecOps

Description

Ensure that Virtual Machine instances have deletion protection enabled.

Instance deletion protection is disabled

Recommendation

Enable deletion protection for the VM instance 'instance-id' in project project-id' to prevent accidental or unauthorized deletion and ensure service availability.

L-2: Instance Default Service Account

Low

Affected Components: projectsproject-id/zones/us-east5-b/instances/instance-id

References: https://cloud.google.com/iam/docs/service-accounts, https://cloud.google.com/iam/docs/best-practices-service-accounts, https://cloud.google.com/compute/docs/access/service-accounts

Google Security Product: SecOps

Description

Ensures that compute instances are not configured to use the default service account.

Default service account is used for instance

Recommendation

Create a dedicated custom service account with the minimum necessary permissions for the 'instance-id' instance. Assign this new custom service account to the instance and ensure the default service account is no longer used. Regularly review and audit the permissions granted to all service accounts.





A Appendix