Report 202200999-1

Security Analysis ZITADEL

Created for ZITADEL on 24. November 2022

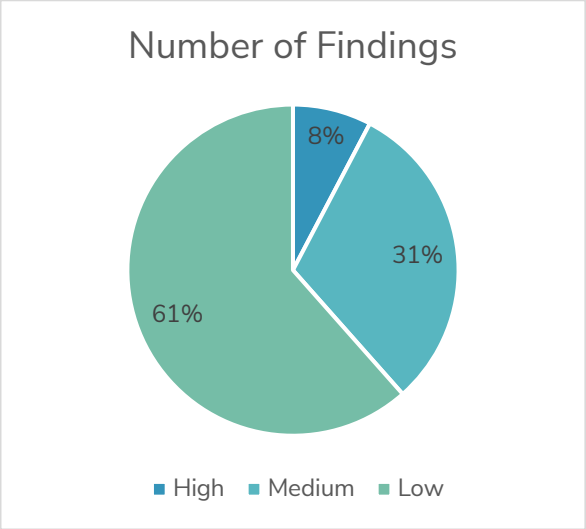
Document-ID: FIS-20220099-1
Version: 1.0
Classification: Confidential
Author: Sven Fassbender

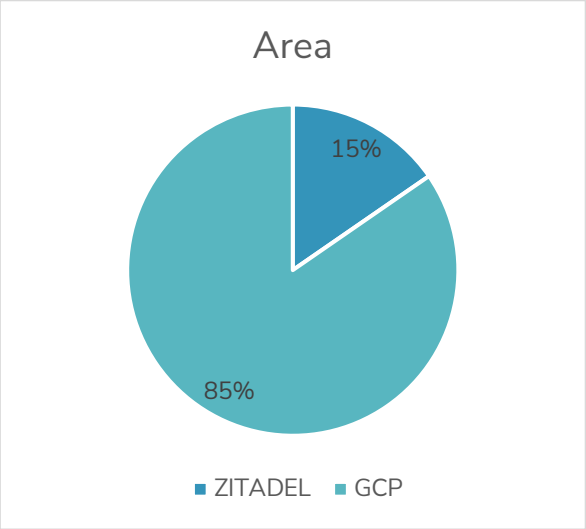
1 CONTENT

2 Management Summary

ZITADEL tasked Fassbender Information Security to perform a security analysis of the ZITADEL IAM service and the cloud hosting configuration. The service is hosted on the Google Cloud Platform and is managed by the customer. All tasks were conducted between August 15, 2022, and August 26, 2022. The tests were performed on the test environment.

During the security analysis one high, four medium and eight low criticality findings were identified. Most of the findings was in the Google Cloud Platform (GCP) configuration.





The high criticality finding describes a missing authorization check on the actions function within ZITADEL. Authenticated users with organization owner permissions were able to grant roles of projects of other organizations on the same ZITADEL instance. This finding was resolved during the security analysis and a patch to the service was published.

The medium criticality findings include insufficient logging and missing monitoring as well as insecure identity and access management configurations on the Google Cloud Platform.

All low criticality findings pose a low risk to the overall security of the system but should be fixed to increase the resilience and to be in line with security best practices.

The overall security level of the ZITADEL service is rated as good.

3 Findings Overview

ID	Finding	Criticality
5.1	Privilege Escalation by Actions	High
5.2	Missing Logging for Firewalls	Medium
5.3	Insufficient Monitoring	Medium
5.4	Basic Roles in Use	Medium
5.5	Service Accounts with Admin Privileges	Medium
5.6	Access to Instance Settings with Role Org Project Creator	Low
5.7	Unnecessary Firewall Rules	Low
5.8	Extensive Firewall Rule	Low
5.9	Cloud Armor Rules	Low
5.10	Unnecessary Bastion Host	Low
5.11	Roles Assigned to Users Instead of Groups	Low
5.12	User Managed Service Account Keys	Low
5.13	Insecure Bucket Configuration	Low

4 Scope

The following test environment was defined as the subject to the analysis:

- https://*.zitadel.app

The contractor created its own ZITADEL instances and examined them in a partly automatic but mostly manual testing procedure. So-called denial-of-service (DoS) or distributed denial-of-service (DDoS) and social engineering attacks were not carried out.

The investigation was based on internationally recognized standards for information security for web applications from the non-profit organization Open Web Application Security Project (OWASP). The analyst focused on the following sub-areas:

- Authentication testing
- Authorization testing
- Auditing of the role and identity concept
- Examination of the implementation of session management
- Resilience of the cryptography used
- Protection of data "at rest
- Protection of data "at transport level
- Protection against injection attacks
- Verification of the configuration of security relevant components
- Checking for configurations and vulnerabilities that favor or result in information leakage

The system architecture was examined for implementation according to the current security best practices. In doing so, it was checked whether the following design guidelines were considered:

- Zero-Trust
- Privacy-by-Design
- Security-by-Design
- Least-Privilege

5 FINDINGS ZITADEL

5.1 Privilege Escalation by Actions

Class	Authorization
Criticality	High
Area	ZITADEL

The Actions feature allows an authorized user with the role "Organization Owner" to add a grant to a new external user for a project within another organizations scope. An attacker can utilize this vulnerability to create/escalate its privileges on another organization's projects.

The new Actions feature of the ZITADEL console allows organization owners to programmatically perform certain functionalities. ZITADEL provides an API that can be utilized by the legitimate user to e.g., extract metadata or add grants for projects. The full API specification can be found here[1].

During the security analysis it was found that the Actions feature can be abused to add grants of a project that is not within the organizations scope. The attacker needs the permissions of an "Organization Owner" (ORG_OWNER) and must be in the possession of the attacked Project-ID as well as the to be assigned roles key value.

The following action was created to add grants to a user of a project within a different scope:

```
function addGrant(ctx, api){
    api.userGrants.push({
    ProjectID: '175051395999727873',
    Roles: ['testkey1']
  });
}
```

The action was then assigned to the flow "External Authentication".

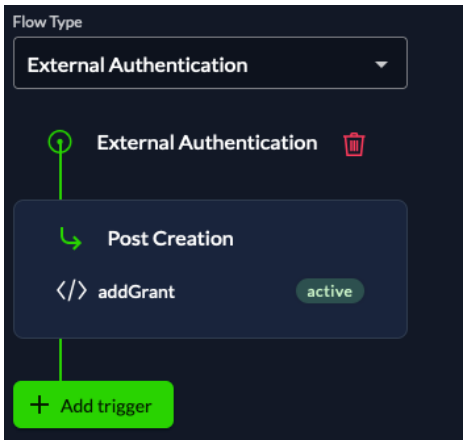


Figure 1 - Screenshot of the final flow, with the malicious action assigned

Once an external user registered to the ZITADEL organization, the grant was assigned.

[1] ZITADEL Documentation, Actions, https://docs.zitadel.com/docs/apis/actions, last visited on August 24, 2022

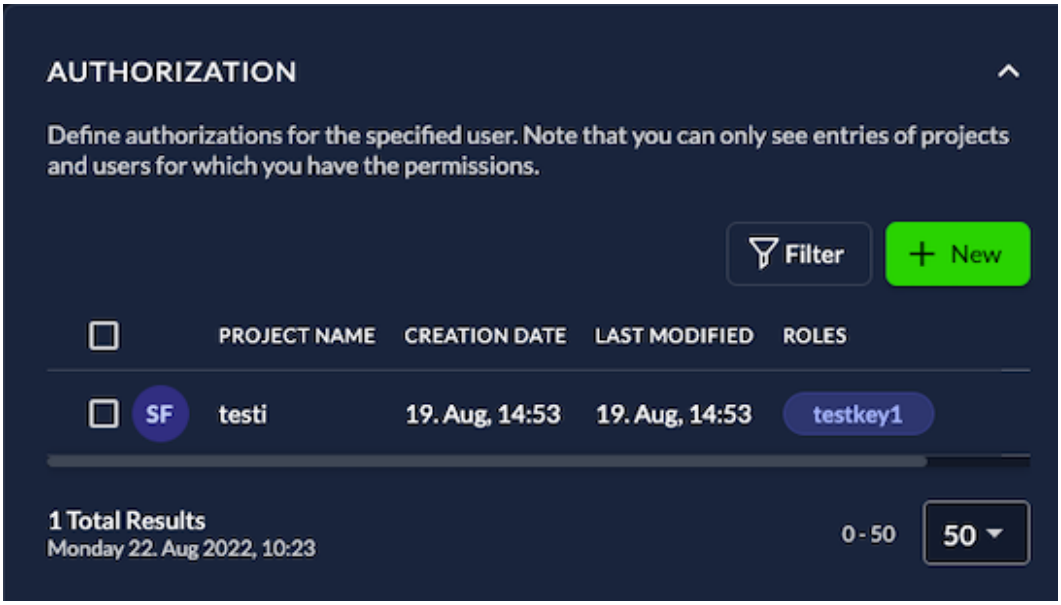


Figure 2 - Screenshot showing the assigned role to the defined project

5.1.1 Recommendation

It is recommended, to limit the actions to the scope of the organization concerned.

5.1.2 Re-Test Result

The finding has been reported to ZITADEL after discovery. Immediate actions were taken to reproduce and discover the source of the vulnerability. Patched versions of ZITADEL were created and a security advisory[2] was published. The finding has been resolved with the following ZITADEL versions:

- 2.x versions are fixed on >= 2.2.0
- 1.x versions are fixed on >= 1.87.1

[2] Security Advisory ZITADEL, Broken Authorizations in ZITADEL Actions, https://github.com/zitadel/zitadel/security/advisories/GHSA-c8fj-4pm8-mp2c, last visited on August 28, 2022

5.2 Missing Logging for Firewalls

Class	Logging and Monitoring
Criticality	Medium
Area	Google Cloud Platform

Logging for existing Firewall rules is deactivated. Policy violations will not be logged and thus cannot be monitored.

ZITADEL infrastructure is hosted in Google Cloud. A Virtual Private Network (VPC) exists to manage and allow the communication between deployed services. Access to and from the VPC is limited by firewall rules. Violations of such a policy, can be an indicator for an attack. Therefore, such violations should be logged and monitored.

During the security analysis it was found that the logging is disabled for all firewall rules in place.

Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network ↑	Logs
default-allow-icmp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	65534	default	Off
default-allow-internal	Ingress	Apply to all	IP ranges: 10.128.0.0/9	tcp:0-65535 udp:0-65535 icmp	Allow	65534	default	Off
default-allow-rdp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:3389	Allow	65534	default	Off
default-allow-ssh	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	65534	default	Off
all-instances-ssh	Ingress	Apply to all	IP ranges: 35.235.240.0/20	tcp:22	Allow	1000	zitadel-cloudrun-network	Off
allow-internal-cockroach	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:26257	Allow	1000	zitadel-cloudrun-network	Off

As no remote management services are activated on the ZITADEL containers, the impact is very limited.

5.2.1 Recommendation

It is recommended, to enable logging for all necessary firewall rules. Furthermore, alerts should be configured to enhance the visibility of rule violations (see finding 5.3).

5.3 Insufficient Monitoring

Class	Logging and Monitoring
Criticality	Medium
Area	Google Cloud Platform

No policies were defined in the Google Cloud Platform to be informed about possible changes or security-relevant incidents. An attacker can apply unnoticed changes or perform attacks on the ZITADEL services.

The Google Cloud Platform offers the option to create metric-based or log-based alerts. These alerts are defined in alerting policies and can be used to e.g., observe the logs for messages. Monitoring and alerting are a recommended control to enhance the visibility of attacks. Actions by humans can be taken once a policy is violated.

During the security analysis it was found that some alerting policies exist, that monitor the latency (performance) of the ZITADEL services. Nevertheless, no policies were defined that track changes in the GCP configuration or observe the log for attack attempts.

An attacker can attack the GCP instance without being noticed. Often an attacker needs to streamline the attack to be successful. In such a case, unsuccessful attempts would remain unnoticed and ZITADEL cannot take proactive actions to stop or mitigate the attacks impact.

5.3.1 Recommendation

It is recommended, it is recommended to create additional policies that track changes and take the Google Cloud Armor logs into account.

5.4 Basic Roles in Use

Class	Identity and Access Management
Criticality	Medium
Area	Google Cloud Platform

Basic Google Cloud Platform roles are assigned, this does not follow security best practices as these roles can have extensive permissions.

Google Cloud Platform comes with default roles that can be assigned to individual users or Google Suite groups. Those roles have extensive permissions on the platform. Depending on the role and the overall setup, these permissions may be extensive. In production environments the default rules should not be assigned, instead custom roles should be created that grant the minimum necessary permissions

During the security analysis it was found that default roles are used and assigned to individual users and service accounts. This applies to the following rules:

- Editor
- Owner

The assigned users have extensive permissions on all Google Cloud services. These permissions can be exploited intentionally, and the risk of a human mistake is increased.

5.4.1 Recommendation

It is recommended, to review the permissions that the individual and service accounts require to perform the necessary actions on the Google Cloud Platform. Custom roles that have these permissions assigned should be created and assigned to Google Suite groups.

5.5 Service Accounts with Admin Privileges

Class	Identity and Access Management
Criticality	Medium
Area	Google Cloud Platform

Custom service accounts have administrative privileges assigned. A compromised service account would have extensive permissions on the assigned services.

In general, the principle of least privileges should be considered when assigning permissions to users or service accounts. This principle states that only required permissions are granted. Allowing a user or service account to perform administrative actions is usually not necessary.

During the security analysis it was found that several user and service accounts have administrative roles assigned. The following roles are affected by this finding:

- Editor
- Storage Admin
- Monitoring Admin

An attacker must be in the possession of an individual user or service account to take advantage of this finding.

5.5.1 Recommendation

It is recommended, to grant the service accounts a minimum of required privileges so that the risk of a compromised user is minimized.

5.6 Access to Instance Settings with Role Org Project Creator

Class	Authorization
Criticality	Low
Area	ZITADEL

An authorized user with the role "Org Project Creator" can read the organization settings. An attacker can use this information to mount further attacks on the system.

The ZITADEL console allows organization owners to grant finely granulated permissions to the registered users. These permissions allow or limit access to certain areas and APIs of the application. The role "Org Project Creator" should only be allowed to create his own projects and the related settings. A user with this role assigned does not require access to the settings of the organization.

During the security analysis it was found that certain API calls, related to the organization settings, were nevertheless allowed to the role "Org Project Creator". The following list shows the affected API calls:

- https://pentest1-ryfeyi.zitadel.app:443/zitadel.management.v1.ManagementService/GetPreviewLabelPolicy
- https://pentest1-ryfeyi.zitadel.app:443/zitadel.management.v1.ManagementService/GetPasswordComplexityPolicy
- https://pentest1-ryfeyi.zitadel.app:443/zitadel.management.v1.ManagementService/GetOIDCInformation
- https://pentest1-ryfeyi.zitadel.app:443/zitadel.management.v1.ManagementService/GetLoginPolicy
- https://pentest1-ryfeyi.zitadel.app:443/zitadel.management.v1.ManagementService/GetLockoutPolicy
- https://pentest1-ryfeyi.zitadel.app:443/zitadel.management.v1.ManagementService/GetLabelPolicy
- https://pentest1-ryfeyi.zitadel.app:443/zitadel.management.v1.ManagementService/GetDomainPolicy
- https://pentest1-ryfeyi.zitadel.app:443/zitadel.management.v1.ManagementService/GetDefaultLoginTexts
- https://pentest1-ryfeyi.zitadel.app:443/zitadel.management.v1.ManagementService/GetDefaultInitMessageText
- https://pentest1-ryfeyi.zitadel.app:443/zitadel.management.v1.ManagementService/GetCustomLoginTexts
- https://pentest1-ryfeyi.zitadel.app:443/zitadel.management.v1.ManagementService/GetCustomInitMessageText

The user can retrieve but not modify the actual settings.

To take advantage of this authorization vulnerability, an attacker must have a user with the role "Org Project Creator".

5.6.1 Recommendation

It is recommended, to follow the information hiding principle. According to this principle the user must not be able to retrieve information of the application, that is not needed to perform his tasks. The authorization controls should be adjusted accordingly.

5.7 Unnecessary Firewall Rules

Class	Security Settings
Criticality	Low
Area	Google Cloud Platform

Unnecessary VPC firewall exist to access remote management ports. This increases the risk of compromised containers.

ZITADEL infrastructure is hosted in Google Cloud. A Virtual Private Network (VPC) exists to manage and allow the communication between deployed services. Extensive ingress or egress firewalls increase the attack surface of the environment and facilitate the process of data exfiltration.

During the security analysis it was found that some VPC firewall rules exist, that are not necessary. The following table shows the rules mentioned:

Name	Type	Protocols/ports	Network
default-allow-rdp	Ingress	tcp:3389	default
default-allow-ssh	Ingress	tcp:22	default
default-allow-internal	Ingress	tcp:0-65535, udp:0-65535	default
default-allow-icmp	Ingress	Icmp	default
all-instances-ssh	Ingress	tcp:22	zitadel-cloudrun-network

The firewall rules allow access to remote management ports, even though the ZITADEL containers do not expose such services.

An attacker must be able to activate remote management services, to take advantage of the security misconfiguration.

As no remote management services are activated on the ZITADEL containers, the impact is very limited.

5.7.1 Recommendation

It is recommended, to delete unnecessary firewall rules. In general, the default network and the existing default firewall rules can be removed.

5.8 Extensive Firewall Rule

Class	Security Settings
Criticality	Low
Area	Google Cloud Platform

Unnecessary VPC firewall exist to access remote management ports. This increases the risk of compromised containers.

ZITADEL infrastructure is hosted in Google Cloud. A Virtual Private Network (VPC) exists to manage and allow the communication between deployed services. Extensive ingress or egress firewalls increase the attack surface of the environment and facilitate the process of data exfiltration.

During the security analysis it was found that some VPC firewall rules exist, that are extensive. The following table shows the rules mentioned:

Name	Type	Protocols/ports	Network
allow-internal-cockroach	Ingress	tcp:26257	zitadel-cloudrun-network

The firewall rules allow access to the cockroach database port without source restrictions.

No cockroach database is exposed on the Google Cloud Platform. Therefore, the impact is limited.

5.8.1 Recommendation

It is recommended, to delete the firewall rule if it is unnecessary. If the policy is required, then source restrictions should be defined.

5.9 Cloud Armor Rules

Class	Security Settings
Criticality	Low
Area	Google Cloud Platform

The Cloud Armor configuration does not contain rules to protect against the OWASP Top 10 risks. Attack attempts cannot be detected, and harmful payloads can reach the ZITADEL services.

Google Cloud Armor offers predefined rules to protect the hosted applications from malicious payloads. Payloads that are in the category of the OWASP Top 10 risks can be detected and filtered utilizing signatures of the ModSecurity Core Rule Set[3] (CSR). It's noteworthy mentioning that the CSR will not prevent all kinds of attacks on its own. Therefore, the ZITADEL services resilience measures are still crucial.

During the analysis it was found that rules exist to prevent DoS and DDoS attacks by limiting the maximum number of requests per time. Nevertheless, the predefined CSR rules were not enabled.

An attacker can send well known malicious payloads to the ZITADEL services. During the security analysis no vulnerability has been identified, that could be exploited by such payloads.

5.9.1 Recommendation

It is recommended, to implement the Core Rule Set within Google's Cloud Armor[4].

[3] OWASP ModSecurity Core Rule Set, https://github.com/coreruleset/coreruleset//, last visited on August 26, 2022

[4] Google Cloud Armor overview, https://cloud.google.com/armor/docs/cloud-armor-overview?hl=en, last visited on August 26, 2022

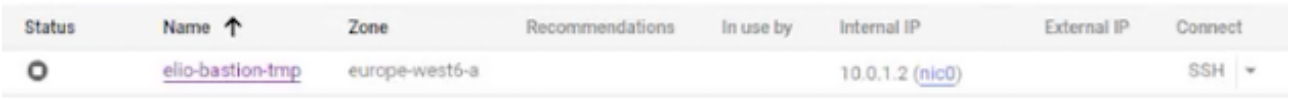
5.10 Unnecessary Bastion Host

Class	Attack Surface
Criticality	Low
Area	Google Cloud Platform

A disabled VM instance is present in the Google Cloud Platform. An attacker may benefit from an extended attack surface, if the VM is enabled but not used.

VM instances on the Google Cloud Platform can be used to deploy custom images. Such images can be downloaded from public sources or can be created individually. The services that are exposed by the images depends on the image itself. It is common practice to reduce the attack surface of cloud and network environments by disabling or removing unnecessary machines.

During the security analysis it was found that a disabled bastion host machine is present in the Google Cloud Platform. An interview with the administrator revealed that the machine will no longer be needed.



Although the risk posed by the deactivated machine is very low. It can be completely deleted for reasons of administrability.

To take advantage of this finding, an attacker must be able to activate the machine (high privileges required) and the attacker must be in the possession of the SSH keys to access the SSH interface.

5.10.1 Recommendation

It is recommended, to remove unneeded machines from the cloud environment to eliminate the existing risks.

5.11 Roles Assigned to Users Instead of Groups

Class	Identity and Access Management
Criticality	Low
Area	Google Cloud Platform

Google Cloud Platform roles are assigned to individual users instead of Google Suite groups. This decreases the administrability of the access management.

Security best practices recommend assigning Google Cloud Platform roles to Google Suite groups instead of to individual users. The reason is, that it is easier to manage the users of a group instead of updating the IAM policy.

During the security analysis it was found that Google Suite groups are not used to manage the roles. This applies to the following rules, that have individual users and service accounts assigned:

- Editor
- Secret Manager Secret Accessor
- Owner

The administrability is decreased by not using Google Suite groups.

5.11.1 Recommendation

It is recommended, to create Google Suite groups e.g., developers, maintainers and so on. The necessary roles can be assigned to these groups and individual users can be added or removed.

5.12 User Managed Service Account Keys

Class	Identity and Access Management
Criticality	Low
Area	Google Cloud Platform

Several service accounts on the Google Cloud Platform have user managed service account keys. The risk of a key theft is increased.

Google Cloud Platform allows users to create and manage their own service account keys. These can be used to authenticate on a service as the respective service account. The key management must be performed manually (key rotation, etc.). Alternatively, GCP can manage the keys, these keys cannot be exported, therefore there are limitations to the usage of such keys e.g., for programmatic purposes. The risk of a service account key theft is increased since user managed keys can be exported.

During the security analysis it was found that several service accounts have user managed keys assigned. The following service accounts are affected by this finding:

- local-livio@zitadel-cloud.iam.gserviceaccount.com
- customer-portal@zitadel-cloud.iam.gserviceaccount.com
- grafana-cloud@zitadel-cloud.iam.gserviceaccount.com
- elio-migration@zitadel-cloud.iam.gserviceaccount.com
- terraform-cloud@zitadel-cloud.iam.gserviceaccount.com

An attacker who gets in the possession of such a user managed key, can impersonate the respective service account.

5.12.1 Recommendation

It is recommended, to review the listed service accounts. If the service accounts keys must be exportable e.g., because the key must be used programmatically a key management should be applied. If the keys can be managed by GCP, the user managed keys should be removed.

5.13 Insecure Bucket Configuration

Class	Security Misconfiguration
Criticality	Low
Area	Google Cloud Platform

A Google Cloud Platform bucket is configured without logging and has versioning disabled. An attacker can benefit from disabled logging and stored data cannot be recovered if overwritten or deleted.

Google Cloud Platform offers versioning and logging capabilities for the cloud storage. Logging is a generally recommended security control to allow reviewing access and storage logs. The versioning feature allows recovery if data has been accidentally or intentionally overwritten or deleted.

During the security analysis it was found that a bucket is configured without logging and versioning enabled. The following bucket is affected by this finding:

- zitadel-app-data

To take advantage of this issue an attacker must be able to access or manipulate data on the cloud storage.

5.13.1 Recommendation

It is recommended, to enable logging and versioning on the listed bucket.

6 VERSIONING

Version	Date	Description	By
0.1	August 17, 2022	Initial version of the report created.	Sven Fassbender
0.2	August 28, 2022	Draft ready for review	Sven Fassbender
0.3	August 29, 2022	Review performed	Sven Fassbender
1.0	September 1, 2022	Report delivery to customer	Sven Fassbender