1. **Misconfigured Google Cloud Storage Bucket Policies**

A Google Cloud Storage service is a public storage service offered by google cloud that enables business to store their data in the bucket.

But if any misconfigured policies are attached to the bucket, then attacker can easily abuse those policy and elevate or escalate privileges onto this bucket which can result in sensitive data exposure.

Attackers View

* Search for the publicly exposed bucket all cloud storage buckets used the same format given below.
* Cloud Storage Bucket URL Format [https://storage.cloud.google.com/BUCKET\_NAME/](https://storage.cloud.google.com/BUCKET_NAME/OBJECT_NAME)
* You can use the below URL for checking all kind of IAM policy attached to the target bucket by replacing the bucket name.

(<https://www.googleapis.com/storage/v1/b/BUCKET_NAME/iam/testPermissions?permissions=storage.buckets.delete&permissions=storage.buckets.get&permissions=storage.buckets.getIamPolicy&permissions=storage.buckets.setIamPolicy&permissions=storage.buckets.update&permissions=storage.objects.create&permissions=storage.objects.delete&permissions=storage.objects.get&permissions=storage.objects.list&permissions=storage.objects.update>)

* Check if any overly permissive permission is attached with the target bucket by which you can escalate the privileges like in the below screenshot.



Defenders View

* Audit your GCP Buckets for public access with **Red-Bucket-GCP** tool mention in tool section.
* Block public access for the buckets that are publicly accessible by enabling the prevent public access option as given below.



* Check all the policies that are attached with the buckets and remove all the overly permissive permissions attached with the buckets.

Tools.

* https://cloud.google.com/storage/docs/gsutil

References

* <https://github.com/ine-labs/GCPGoat>
* <https://threatpost.com/google-cloud-buckets-exposed-misconfiguration/159429/>