UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00043

MISCONFIGURATION IN GOOGLE CLOUD BUCKETS

DATE ISSUED: 28th September 2020

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

As many as 6% of all Google Cloud buckets have misconfigurations that leave them open to the public, meaning all sensitive information stored within is vulnerable to data leak and misuse by threat actors.

BREAKDOWN

Comparitech have conducted a survey across 2,064 Google Cloud Buckets and discovered that 131 were vulnerable to attack due to misconfiguration. When applied to the total number of Google Cloud Buckets in existence, that 6% may be susceptible to unauthorised access where anything may be uploaded or downloaded from these containers. Of the information stored within these environments, the sensitive data recovered by the group included passports, birth certifications, personal profile information of children, server credentials, chat logs and source code.

The naming conventions specified by Google mean that often, these database repositories are not difficult to find. Comparitech were able to locate 2,000 buckets within 2.5hours, with no prior knowledge of their existence.

While this study focused solely on Google Cloud Buckets, it has highlighted the need to check Cloud configuration across all providers to ensure your data is kept securely locked away from prying eyes, particularly as we increase our reliance on Cloud services.

REMEDIATION STEPS

- Scan the web using tools to find out whether your bucket is open to the public – Comparitech have a few recommendations on their website below
- Using Google's security guidance for Cloud Buckets, perform the following steps: turn on uniform bucket-level access and its org policy, enable domain-restricted sharing, add encryption to cloud stored data with Cloud KMS and secure your data with VPC Service Controls. It is also recommended that you audit cloud storage with Cloud Audit Logging.

REFERENCES & RESOURCES

Comparitech:	https://www.comparitech.com/blog/information-security/google-cloud-buckets-unauthorized-access-report/
Google Cloud:	https://cloud.google.com/blog/products/identity-security/find-and-fix-misconfigurations-in-your-google-cloud-resources