RedLock

ALERT: AWS S3 Buckets Should Not Allow 'Authenticated Users Group’

Date Published: April 5, 2017

Summary

Researchers (most notably Chris Vickery) have discovered that a common misconfiguration in Amazon Web Services Simple Storage Service (AWS S3) may expose sensitive enterprise data to unauthorized access. They were actively searching for AWS S3 buckets which were granting access to “Any authenticated AWS users”. These efforts resulted in the exposure of several dozen databases belonging to large financial, healthcare, and technology companies.

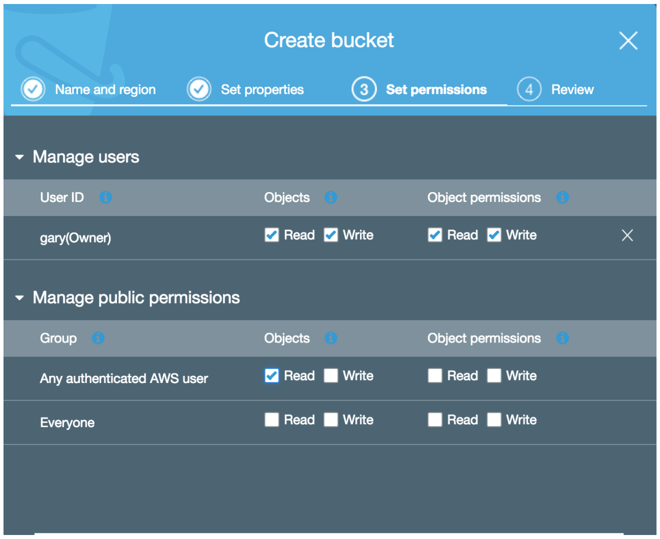
Why you should care?

Researchers are still actively looking for additional databases that may be exposed due to this common misconfiguration and it is only a matter of time before they find them. It is prudent for you to immediately assess your own infrastructure for this vulnerability.

Background

AWS S3 is a simple web service interface that allows organizations to easily store and retrieve data. S3 is used for backups, application hosting, file server, and media and software delivery. Given its ease of use, S3 has become an attractive option for organizations to store large amounts of data in it.

Access to S3 is managed through Access Control Lists (ACL) where customers specify which users are permitted access to the buckets. It is a good security practice to make sure that these ACLs only allow specific authorized internal users to have access to the data in the S3 buckets. But often, AWS administrators grant access to “Any authenticated AWS users” (see the image below) thinking that this access permission will only allow internal users to access data in the S3 buckets. This is a common misconception as this permission grants S3 access to ANY user with valid AWS credentials and exposes sensitive enterprise data to unauthorized external access. With this access permission, a malicious user simply needs to figure out the name of the bucket and/or the files inside the bucket. Once they have this information, they can easily make API calls to the S3 bucket with their valid user credentials and gain access to highly sensitive enterprise data.



Manage users

User ID	Objects	Object permissions
gary(Owner)	☑ Read ☑ Write	☑ Read ☑ Write

Manage public permissions

Group	Objects	Object permissions
Any authenticated AWS user	☑ Read □ Write	□ Read □ Write
Everyone	□ Read □ Write	□ Read □ Write

Remediation

1. Make sure that the ACL for your S3 buckets are as restrictive as possible, especially those that contain highly sensitive enterprise data. Only a handful of authorized internal users should have access to the S3 buckets.
2. Use the “Any authenticated AWS user” permission for a very narrow set of B2B use cases where it’s necessary to expose some of the data to any and all AWS customers.
3. Due to the dynamic nature of cloud infrastructure, it is often impossible to enforce uniform security policy across the different DevOps teams in your organization. Make sure you have a security tool in place that continuously monitors S3 buckets and other cloud workloads, sends contextual alerts, and auto-remediates when such security incidents are discovered.