|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | AWS S3 Access Misconfigurations | | |
| **Findings Categorization** | | | | |
| **Business Impact** | | Medium | **CVSS v4.0 Score** | 7.0 (High) |
| **CVSS Vector** | | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N | | |

Technical Description

Improperly configured AWS S3 buckets can expose sensitive data publicly, allowing attackers to access, download, or modify files without authentication. While there might be a legitimate business need for S3 bucket exposures, i.e. serving static websites – oftentimes these could be misconfigured to contain sensitive files or data.

During this engagement, engineers discovered that the bucket **dev.huge-logistics.com** publicly listable and contained sensitive files including website content, migration files, and administrative exports. These misconfigurations allowed privilege escalation from unauthenticated S3 access to **full administrative access to highly sensitive organizational data.**

Business Impact Description

Exposure of hardcoded AWS credentials combined with publicly accessible S3 content represents a severe risk to the security posture of the business. In this scenario, successful access allowed retrieval of sensitive files containing PII, financial data, and administrative credentials, which could be leveraged to further attack internal systems, access cloud workloads, or impersonate privileged users. The level of access that can be easily gained undermines the confidentiality, integrity, and availability of organizational data and infrastructure.

Affected Systems

**Endpoint:** https://dev.huge-logistics.com.s3.amazonaws.com/

**S3 Bucket:** s3://dev.huge-logistics.com

* s3://dev.huge-logistics.com/admin/
* s3://dev.huge-logistics.com/migration-files/
* s3://dev.huge-logistics.com/shared/

Steps to Reproduce

During external enumeration, engineers identified and queried the S3 bucket the shared/hl\_migration\_project.zip archive was retrieved and extracted, revealing a PowerShell script containing hardcoded AWS credentials. These credentials were valid and allowed authenticated access to the bucket’s sensitive directories, including /admin and /migration-files/.

/Screenshot 1

Caption 1: Successful retrieval of the .zip file stored in the /shared directory, with the archive containing a script with hardcoded AWS credentials.

Engineers then leveraged these obtained credentials to widen their access into the client’s cloud environment by utilizing them to authenticate as the `pam-test` user. Enumerating access, engineers were able to access /admin and /migration directories with the `pam-test` user credentials.

TODO

Mitigations

* Immediately rotate and revoke exposed AWS credentials.
* Remove hardcoded credentials from scripts; use AWS Secrets Manager or IAM roles.
* Audit S3 bucket policies to restrict public access; use least privilege permissions.
* Enable AWS CloudTrail logging for all S3 operations.
* Enforce encryption at rest and in transit for sensitive files, encrypt the shared .zip files with a strong, random password – avoid sharing sensitive files through S3 bucket.
* Implement monitoring and alerting for unauthorized access attempts.

References

* **AWS S3 Security Best Practices**
  + https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html
* **MITRE ATT&CK – T1530: Data from Cloud Storage Object**
  + https://attack.mitre.org/techniques/T1530/
* **OWASP – Cloud Security Cheat Sheet:**
  + https://cheatsheetseries.owasp.org/cheatsheets/Cloud\_Security\_Cheat\_Sheet.html