AWS Prowler Failed Finding

Risk is the possibility that something bad could happen that might hurt a company, a system, or people. In cybersecurity, risk happens when there is a weakness (called a vulnerability) in a system that could be attacked by a threat.

Risk is like leaving your front door unlocked in a bad neighborhood. The unlocked door is the vulnerability, and the threat is someone who might break in.

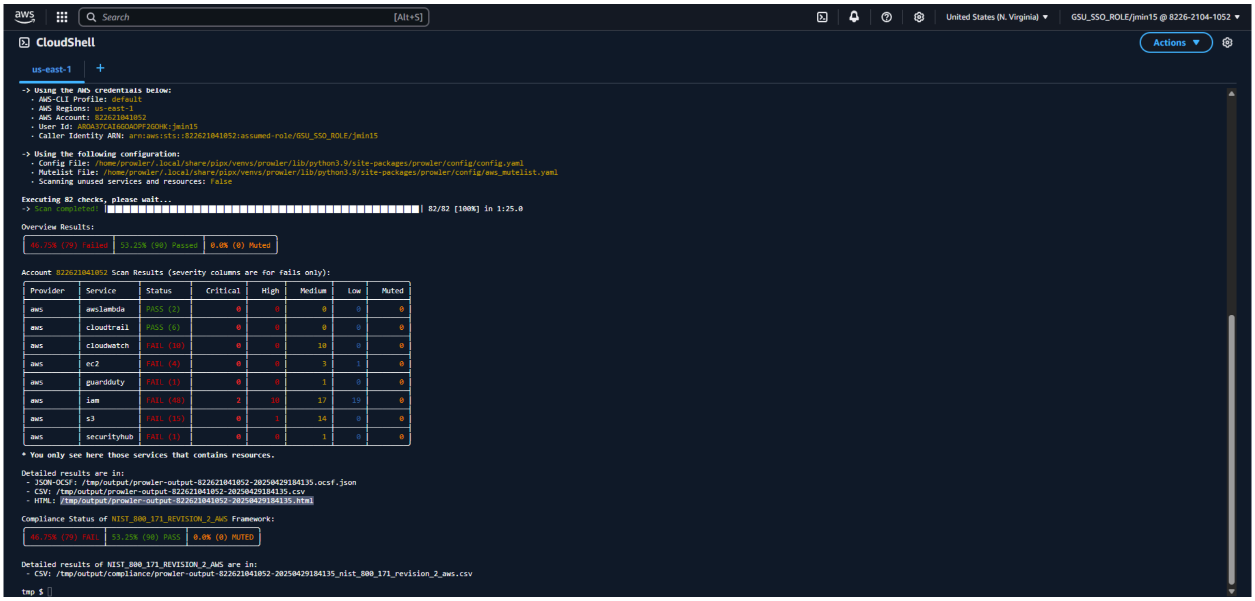
1. *Likelihood* – How likely is it that something bad will happen?
2. *Impact* – How bad would it be if it did happen?

Probable	Critical	Critical	Critical	Critical
Possible	Major	Critical	Critical	Critical
Unlikely	Moderate	Major	Critical	Critical
Rare	Minor	Moderate	Major	Critical
	Low	Medium	High	Very High

X-Axis: Impact

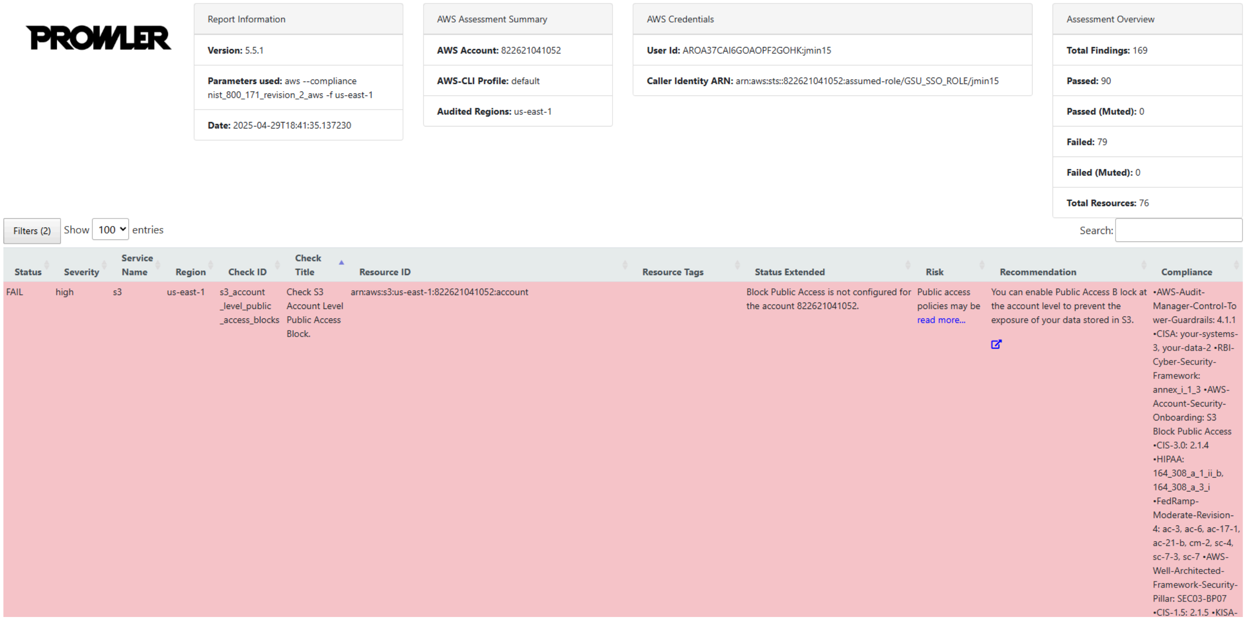
Y-Axis: Likelihood/Proabability

Risk = Likelihood x Impact



aws
Search [Alt+S]
United States (N. Virginia) ▾
GSU_SSO_ROLE/jmin15 @ 8226-2104-1052 ▾
CloudShell
Actions ▾
us-east-1
+

```
-> Using the AWS credentials below:
  · AWS-CLI Profile: default
  · AWS Regions: us-east-1
  · AWS Account: 822621041052
  · User Id: AROA37CAI6GOAOPF2GOHK:jmin15
  · Caller Identity ARN: arn:aws:sts::822621041052:assumed-role/GSU_SSO_ROLE/jmin15

-> Using the following configuration:
  · Config File: /home/prowler/.local/share/pipx/venvs/prowler/lib/python3.9/site-packages/prowler/config/config.yaml
  · Mutelist File: /home/prowler/.local/share/pipx/venvs/prowler/lib/python3.9/site-packages/prowler/config/aws_mutelist.yaml
  · Scanning unused services and resources: False

Executing 82 checks, please wait...
-> Scan completed! |████████████████████████████████████████| 82/82 [100%] in 1:25.0

Overview Results:
╭────────────────────┬─────────────────────┬────────────────╮
│ 46.75% (79) Failed │ 53.25% (90) Passed │ 0.0% (0) Muted │
╰────────────────────┴─────────────────────┴────────────────╯

Account 822621041052 Scan Results (severity columns are for fails only):
╭────────────┬─────────────┬───────────┬────────────┬────────┬──────────┬───────┬─────────╮
│ Provider   │ Service     │ Status    │   Critical │   High │   Medium │   Low │   Muted │
├────────────┼─────────────┼───────────┼────────────┼────────┼──────────┼───────┼─────────┤
│ aws        │ awslambda   │ PASS (2)  │          0 │      0 │        0 │     0 │       0 │
├────────────┼─────────────┼───────────┼────────────┼────────┼──────────┼───────┼─────────┤
│ aws        │ cloudtrail  │ PASS (6)  │          0 │      0 │        0 │     0 │       0 │
├────────────┼─────────────┼───────────┼────────────┼────────┼──────────┼───────┼─────────┤
│ aws        │ cloudwatch  │ FAIL (10) │          0 │      0 │       10 │     0 │       0 │
├────────────┼─────────────┼───────────┼────────────┼────────┼──────────┼───────┼─────────┤
│ aws        │ ec2         │ FAIL (4)  │          0 │      0 │        3 │     1 │       0 │
├────────────┼─────────────┼───────────┼────────────┼────────┼──────────┼───────┼─────────┤
│ aws        │ guardduty   │ FAIL (1)  │          0 │      0 │        1 │     0 │       0 │
├────────────┼─────────────┼───────────┼────────────┼────────┼──────────┼───────┼─────────┤
│ aws        │ iam         │ FAIL (48) │          2 │     10 │       17 │    19 │       0 │
├────────────┼─────────────┼───────────┼────────────┼────────┼──────────┼───────┼─────────┤
│ aws        │ s3          │ FAIL (15) │          0 │      1 │       14 │     0 │       0 │
├────────────┼─────────────┼───────────┼────────────┼────────┼──────────┼───────┼─────────┤
│ aws        │ securityhub │ FAIL (1)  │          0 │      0 │        1 │     0 │       0 │
╰────────────┴─────────────┴───────────┴────────────┴────────┴──────────┴───────┴─────────╯
* You only see here those services that contains resources.

Detailed results are in:
 - JSON-OCSF: /tmp/output/prowler-output-822621041052-20250429184135.ocsf.json
 - CSV: /tmp/output/prowler-output-822621041052-20250429184135.csv
 - HTML: /tmp/output/prowler-output-822621041052-20250429184135.html

Compliance Status of NIST_800_171_REVISION_2_AWS Framework:
╭──────────────────┬───────────────────┬────────────────╮
│ 46.75% (79) FAIL │ 53.25% (90) PASS │ 0.0% (0) MUTED │
╰──────────────────┴───────────────────┴────────────────╯

Detailed results of NIST_800_171_REVISION_2_AWS are in:
 - CSV: /tmp/output/compliance/prowler-output-822621041052-20250429184135_nist_800_171_revision_2_aws.csv

tmp $
```



Report Information

Version: 5.5.1

Parameters used: aws --compliance nist_800_171_revision_2_aws -f us-east-1

Date: 2025-04-29T18:41:35.137230

AWS Assessment Summary

AWS Account: 822621041052

AWS-CLI Profile: default

Audited Regions: us-east-1

AWS Credentials

User Id: AROA37CAI6GOAOPF2GOHK:jmin15

Caller Identity ARN: arn:aws:sts::822621041052:assumed-role/GSU_SSO_ROLE/jmin15

Assessment Overview

Total Findings: 169

Passed: 90

Passed (Muted): 0

Failed: 79

Failed (Muted): 0

Total Resources: 76

Status	Severity	Service Name	Region	Check ID	Check Title	Resource ID	Resource Tags	Status Extended	Risk	Recommendation	Compliance
FAIL	high	s3	us-east-1	s3_account_level_public_access_blocks	Check S3 Account Level Public Access Block.	arn:aws:s3:us-east-1:822621041052:account		Block Public Access is not configured for the account 822621041052.	Public access policies may be read more...	You can enable Public Access B lock at the account level to prevent the exposure of your data stored in S3.	•AWS-Audit-Manager-Control-Tower-Guardrails: 4.1.1 •CISA: your-systems-3, your-data-2 •RBI-Cyber-Security-Framework: annex_i_1_3 •AWS-Account-Security-Onboarding: S3 Block Public Access •CIS-3.0: 2.1.4 •HIPAA: 164_308_a_1_ii_b, 164_308_a_3_i •FedRamp-Moderate-Revision-4: ac-3, ac-6, ac-17-1, ac-21-b, cm-2, sc-4, sc-7-3, sc-7 •AWS-Well-Architected-Framework-Security-Pillar: SEC03-BP07 •CIS-1.5: 2.1.5 •KISA-

Risk Explanation:

Control: Block Public Access is not configured for the account 822621041052.
Platform: AWS
Service: S3
Criticality: High

What is the Risk?

"Public access policies may be applied to sensitive data buckets".When S3 buckets are publicly accessible, data can be exposed to unauthorized users. Essentially, anyone on the internet could access sensitive files if they're not properly restricted. This is especially dangerous if:

- The bucket contains PII, internal documentation, configuration files, or credentials.
- The bucket is used in production and hasn't been properly configured.

Likelihood:

- High : Misconfigured S3 buckets are one of the most common cloud misconfigurations, and attackers routinely scan for them.

Impact:

- High : If exposed data is sensitive or regulated, the fallout can be severe.

Risk Equation:

Risk = Threat x Vulnerability x Impact

- Threat = Data breach or external attack
- Vulnerability = Improper access control on S3 buckets
- Impact = High (ex. data breach, compliance failure, financial loss, reputational damage)

The recommended risk mitigation type is Avoidance (secondary: Reduction).

The organization can avoid the risk of S3 data exposure by enforcing the S3 Public Access Block setting at the account level. This setting, in combination with regular access reviews and proper IAM policies, also reduces the likelihood of misconfigurations and unauthorized access. If full avoidance is not possible, such as if a bucket must be public, then other strategies such as specefic access controls, monitoring, and logging can help reduce risk.

This solution is suggested because instead of having to check every individual bucket's permissions, enabling account-level Public Access Block applies the restriction globally. It:

- Prevents accidental or malicious data exposure
- Simplifies security administration
- Aligns with major compliance frameworks
- Avoids a high-likelihood, high-impact vulnerability

The NIST 800-171 controls found violated were:

Control Families / (Controls):

- 3_1 : Access Controls (3_1_1, 3_1_2, 3_1_3, 3_1_14, 3_1_20)
- 3_3 : Audit and Accountability (3_3_8)
- 3_4 : Configuration Management (3_4_6)
- 3_13 : System and Communications Protection (3_13_5)

Is this finding mapped to other Frameworks?

Yes, this finding is mapped to multiple security frameworks:

- Is this finding mapped to NIST 800-53? Yes
- Is this finding mapped to ISO 27001:2013? Yes
- Is this finding mapped to SOC2? No

Mitigation Plan and Remediation Schedule:

The mitigation plan for the S3 public access misconfiguration involves immediately disabling public access for all S3 buckets by enabling S3 Block Public Access at both the account and bucket level. A thorough review of current S3 permissions, including Access Control Lists and bucket policies, should be done to ensure they follow the least privilege principle. AWS CloudTrail should also be enabled for logging access requests, and CloudWatch Alarms should be set up to detect unauthorized access attempts.

In the short term, ensure server-side encryption is enabled for all sensitive data stored in S3 and perform vulnerability scanning to detect any other misconfigurations. IAM roles and policies should be reviewed and updated to ensure the least privilege. Security awareness training should be conducted for the team on cloud security best practices.

For the long term, implement AWS Config Rules to automatically block public access for new S3 buckets and establish a process for regular audits of S3 configurations, ACLs, and policies. Integrating S3 access logs into a SIEM for continuous monitoring will provide ongoing protection, while penetration testing or red teaming exercises should be performed to uncover vulnerabilities.

This approach will ensure that the S3 environment is secure, compliant, and protected from future misconfigurations.

Compliance Framework and NIST 800-171 Deepdive

A compliance framework is a structured set of guidelines and best practices that organizations use to ensure they meet legal, regulatory, and industry-specific requirements. These frameworks help businesses establish and maintain proper policies, controls, and procedures to manage risks related to data security, privacy, and operations. By following a compliance framework, organizations can demonstrate accountability, maintain customer trust, and avoid legal penalties. Common examples include NIST 800-171 for protecting controlled unclassified information, ISO/IEC 27001 for information security management systems, and SOC 2 for evaluating service providers' data handling practices. Overall, a compliance framework serves as a foundation for maintaining security, promoting transparency, and aligning organizational practices with recognized standards.

NIST 800-171 is a cybersecurity framework developed by the National Institute of Standards and Technology that focuses on protecting controlled unclassified information in non-federal systems and organizations. Its primary goal is to ensure that sensitive government data remains secure when handled by contractors, universities, or private companies working with federal agencies. The framework emphasizes confidentiality and provides a set of structured security requirements tailored for environments outside of the federal government. These requirements are organized into 14 control families, each covering a critical area of cybersecurity. The control families include

- Access Control
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment
- System and Communications Protection
- System and Information Integrity.

These NIST 800-171 families outline 110 specific controls that organizations must implement to protect CUI. These controls provide steps for managing access, monitoring activity, protecting data, responding to threats, and maintaining the integrity of systems. By following these controls, organizations can adhere to compliance and significantly reduce their risk exposure.