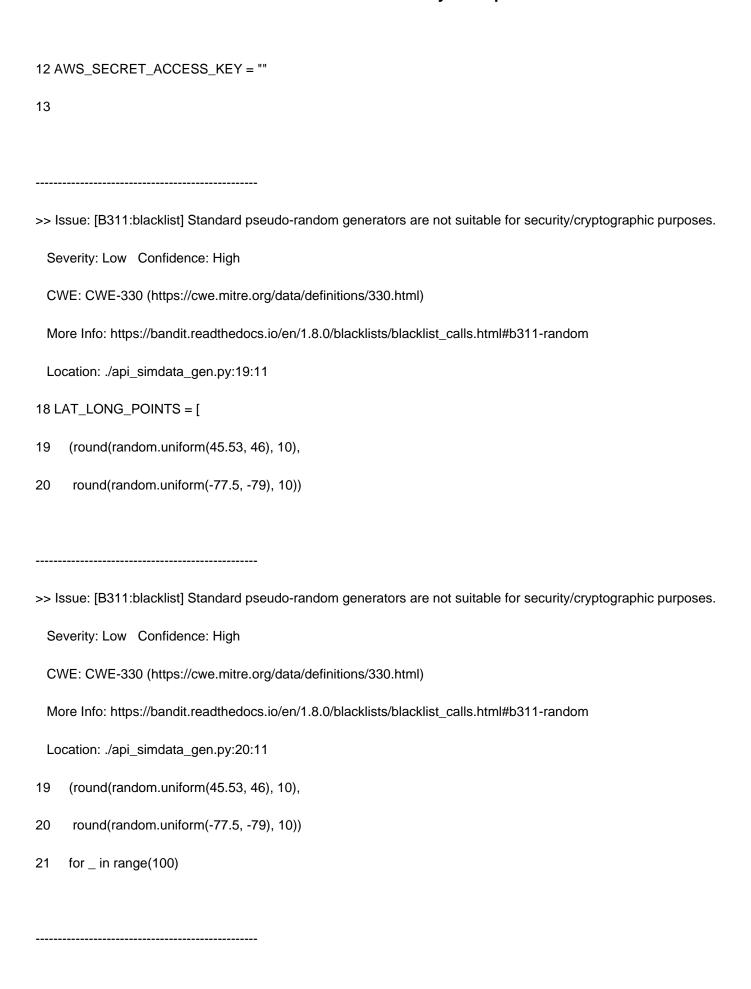
Bandit Report

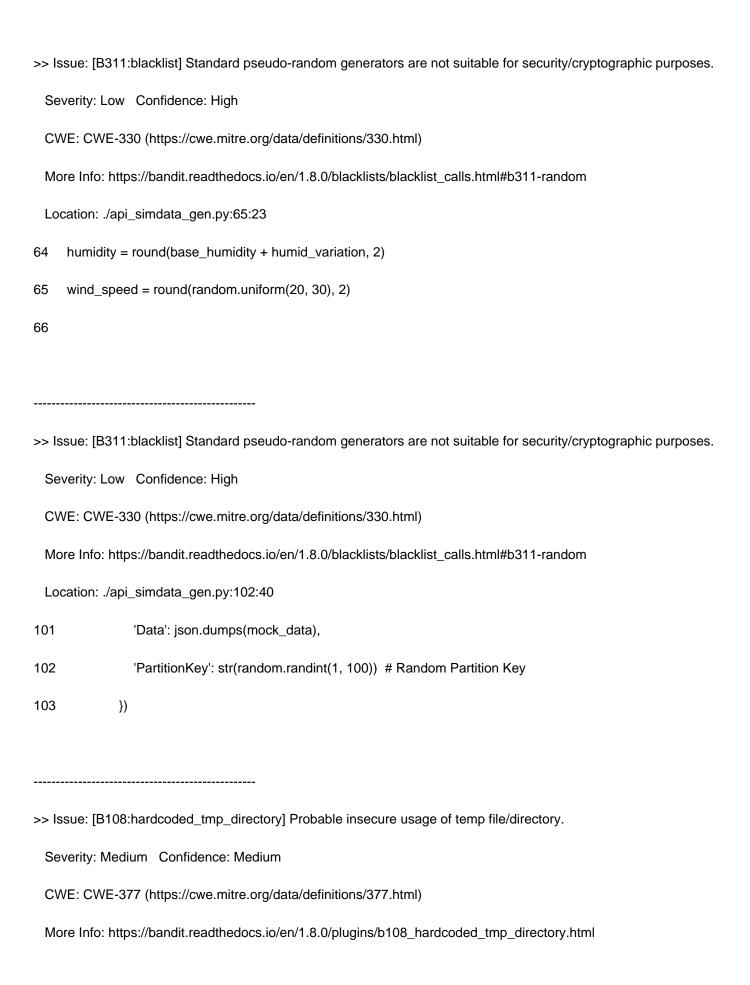
Run	started	1.2024-	12-09	23.20.2	29.296446

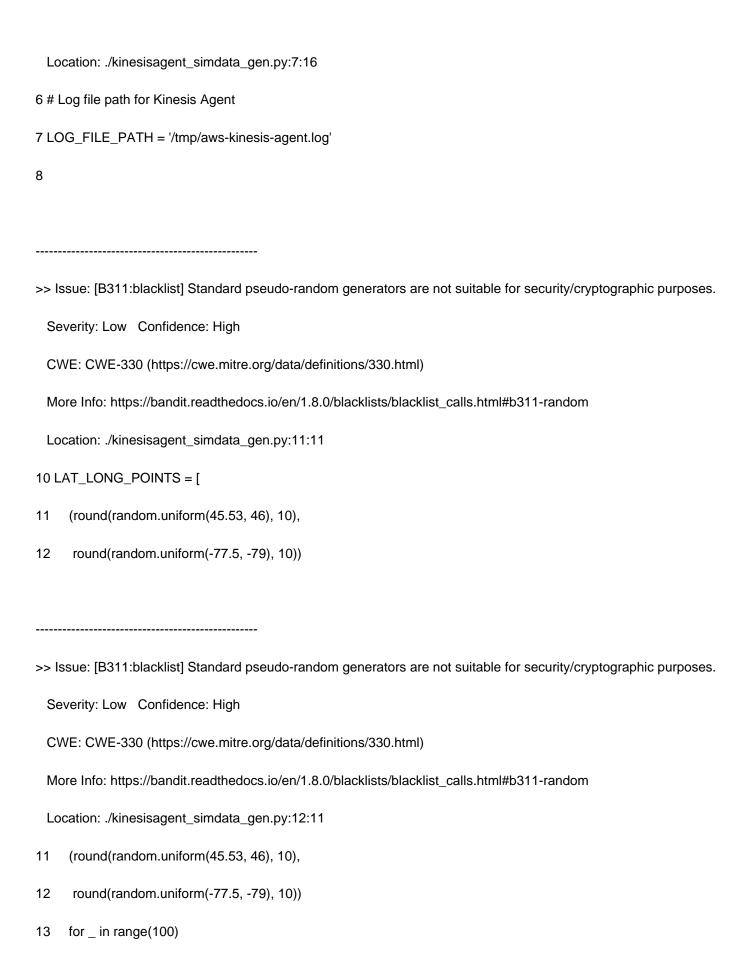
Location: ./api_simdata_gen.py:12:24

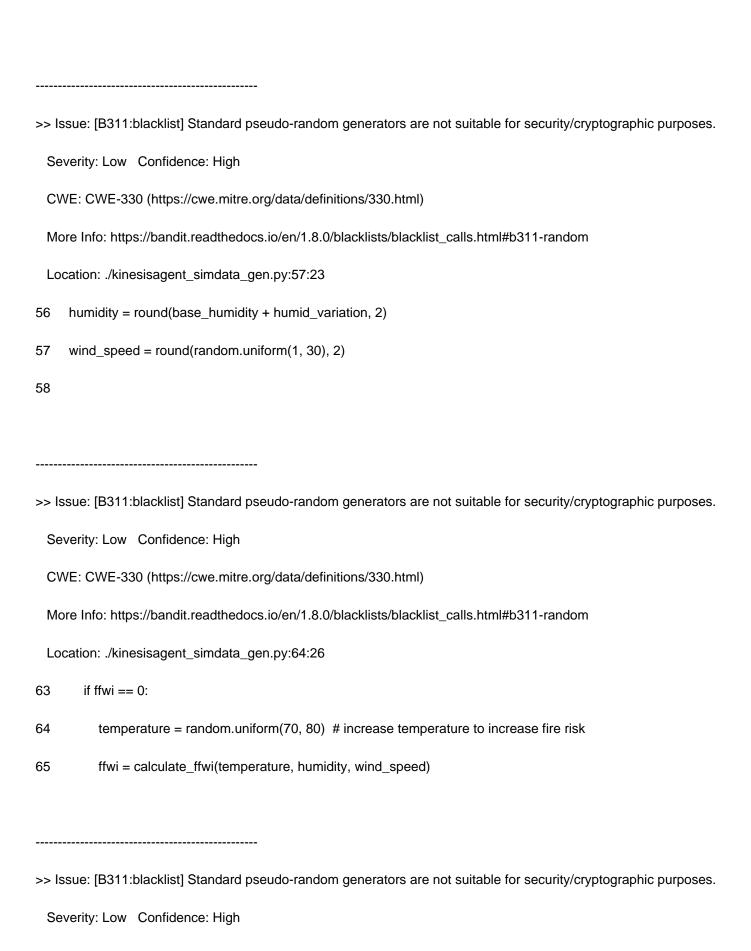
11 AWS_ACCESS_KEY_ID = ""

Test results: >> Issue: [B608:hardcoded_sql_expressions] Possible SQL injection vector through string-based query construction. Severity: Medium Confidence: Low CWE: CWE-89 (https://cwe.mitre.org/data/definitions/89.html) More Info: https://bandit.readthedocs.io/en/1.8.0/plugins/b608_hardcoded_sql_expressions.html Location: ./Lambda_PushToAthena.py:69:12 68 # Step 2: Define the Athena query (make sure to adjust the query based on your table and columns) query = f""" 69 SELECT * 70 71 FROM "default"."forest_weather_data_parquet" 72 WHERE year = '{year}' AND month = '{month}' AND day = '{day}' 73 74 >> Issue: [B105:hardcoded_password_string] Possible hardcoded password: " Severity: Low Confidence: Medium CWE: CWE-259 (https://cwe.mitre.org/data/definitions/259.html) More Info: https://bandit.readthedocs.io/en/1.8.0/plugins/b105_hardcoded_password_string.html









CWE: CWE-330 (https://cwe.mitre.org/data/definitions/330.html) More Info: https://bandit.readthedocs.io/en/1.8.0/blacklists/blacklist_calls.html#b311-random Location: ./kinesisagent_simdata_gen.py:91:44 90 'Data': json.dumps(mock_data), 91 'PartitionKey': str(random.randint(1, 100)) # Random Partition Key 92 }) >> Issue: [B404:blacklist] Consider possible security implications associated with the subprocess module. Severity: Low Confidence: High CWE: CWE-78 (https://cwe.mitre.org/data/definitions/78.html) More Info: https://bandit.readthedocs.io/en/1.8.0/blacklists/blacklist_imports.html#b404-import-subprocess Location: ./static_code_analysis.py:3:0 2 from bandit.core import config as bandit_config 3 import subprocess 4 import os >> Issue: [B607:start_process_with_partial_path] Starting a process with a partial executable path Severity: Low Confidence: High CWE: CWE-78 (https://cwe.mitre.org/data/definitions/78.html) More Info: https://bandit.readthedocs.io/en/1.8.0/plugins/b607_start_process_with_partial_path.html Location: ./static_code_analysis.py:14:0 13 # Run Bandit on the directory

14 subprocess.run(["bandit", "-r", target_directory, "-f", "txt", "-o", output_file])
15
>> Issue: [B603:subprocess_without_shell_equals_true] subprocess call - check for execution of untrusted input
Severity: Low Confidence: High
CWE: CWE-78 (https://cwe.mitre.org/data/definitions/78.html)
More Info: https://bandit.readthedocs.io/en/1.8.0/plugins/b603_subprocess_without_shell_equals_true.html
Location: ./static_code_analysis.py:14:0
13 # Run Bandit on the directory
4 subprocess.run(["bandit", "-r", target_directory, "-f", "txt", "-o", output_file])
15
Code scanned:
Total lines of code: 466
Total lines skipped (#nosec): 0
Total potential issues skipped due to specifically being disabled (e.g., #nosec BXXX): 0
Run metrics:
Total issues (by severity):
Undefined: 0
Low: 13

Medium: 2	
High: 0	
Total issues (by confidence):	
Undefined: 0	
Low: 1	
Medium: 2	
High: 12	
Files skipped (0):	