Security Vulnerability Assessment Report

Executive Summary

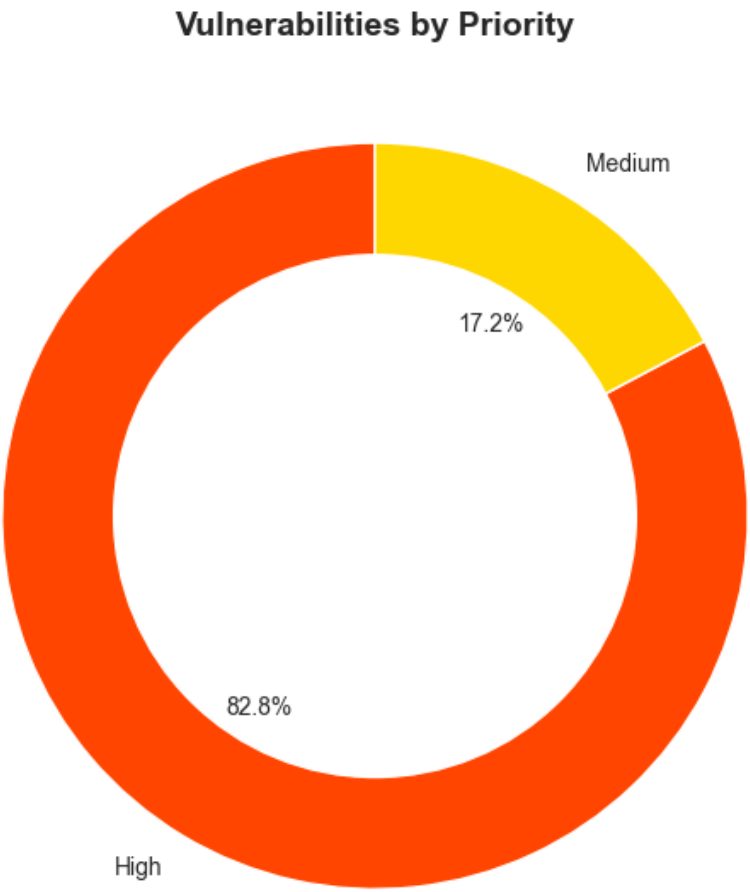
This report presents the findings of a security vulnerability assessment conducted on the data-ingest-monitoring project. A total of 29 vulnerabilities were identified, with 24 classified as high priority. The assessment revealed several critical security issues that require immediate attention, including improper access controls, hard-coded secrets, and insecure configurations.

Key Findings

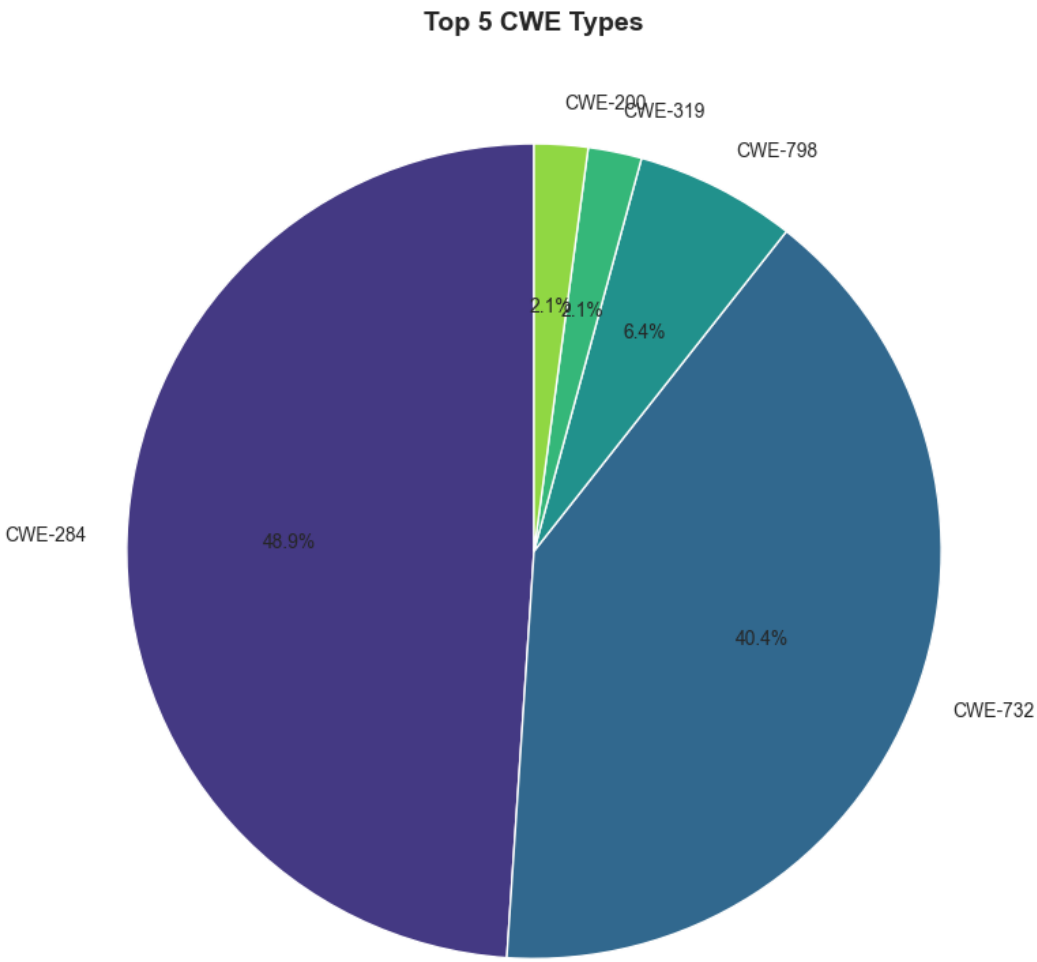
1. 23 instances of improper access control (CWE-284) vulnerabilities
2. 3 instances of hard-coded credentials (CWE-798)
3. 19 instances of incorrect permission assignments (CWE-732)
4. Average CVSS score across filtered vulnerabilities: 7.8
5. Most affected component: cform
6. 24 High priority vulnerabilities
7. 0 vulnerabilities with Critical CVSS score (9.1-10)
8. 24 vulnerabilities with High CVSS score (7.0-9)

Vulnerability Distribution

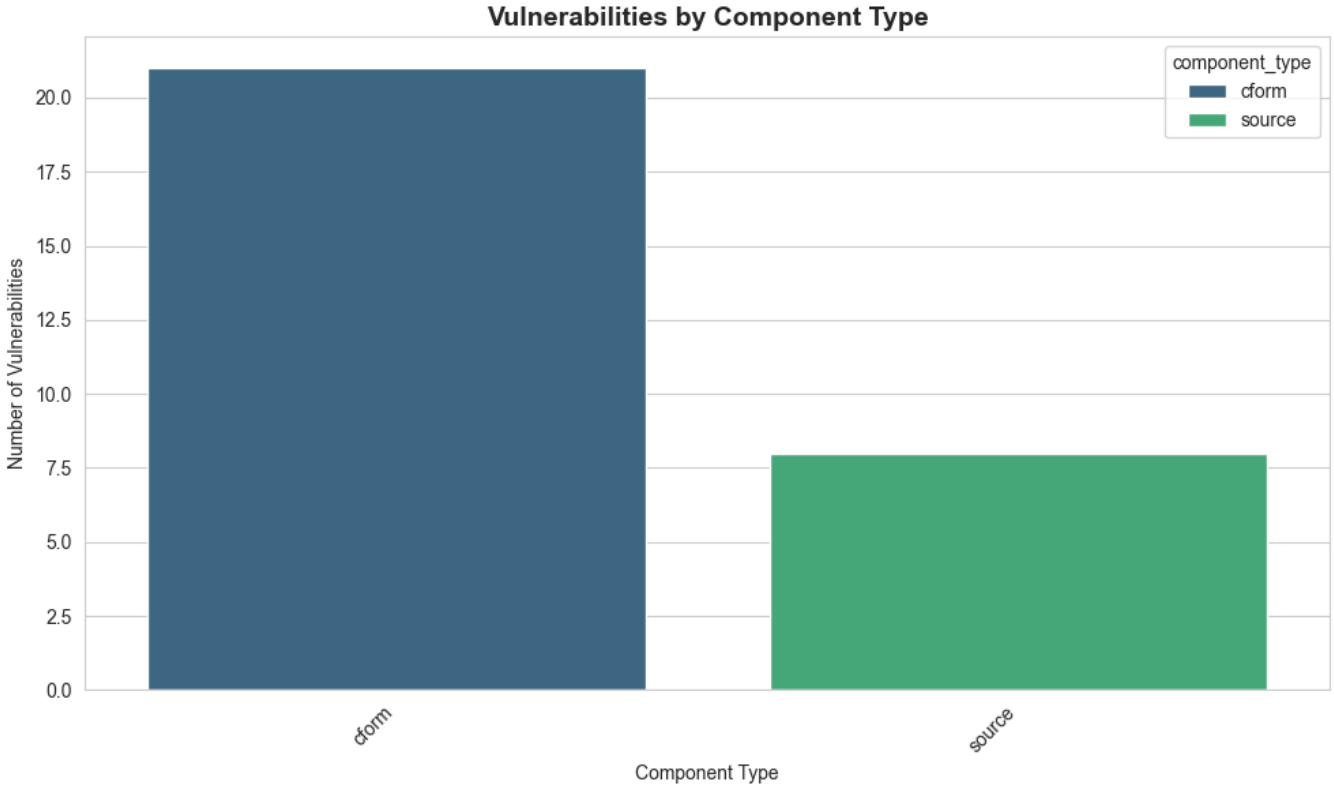
Security Vulnerability Assessment Report

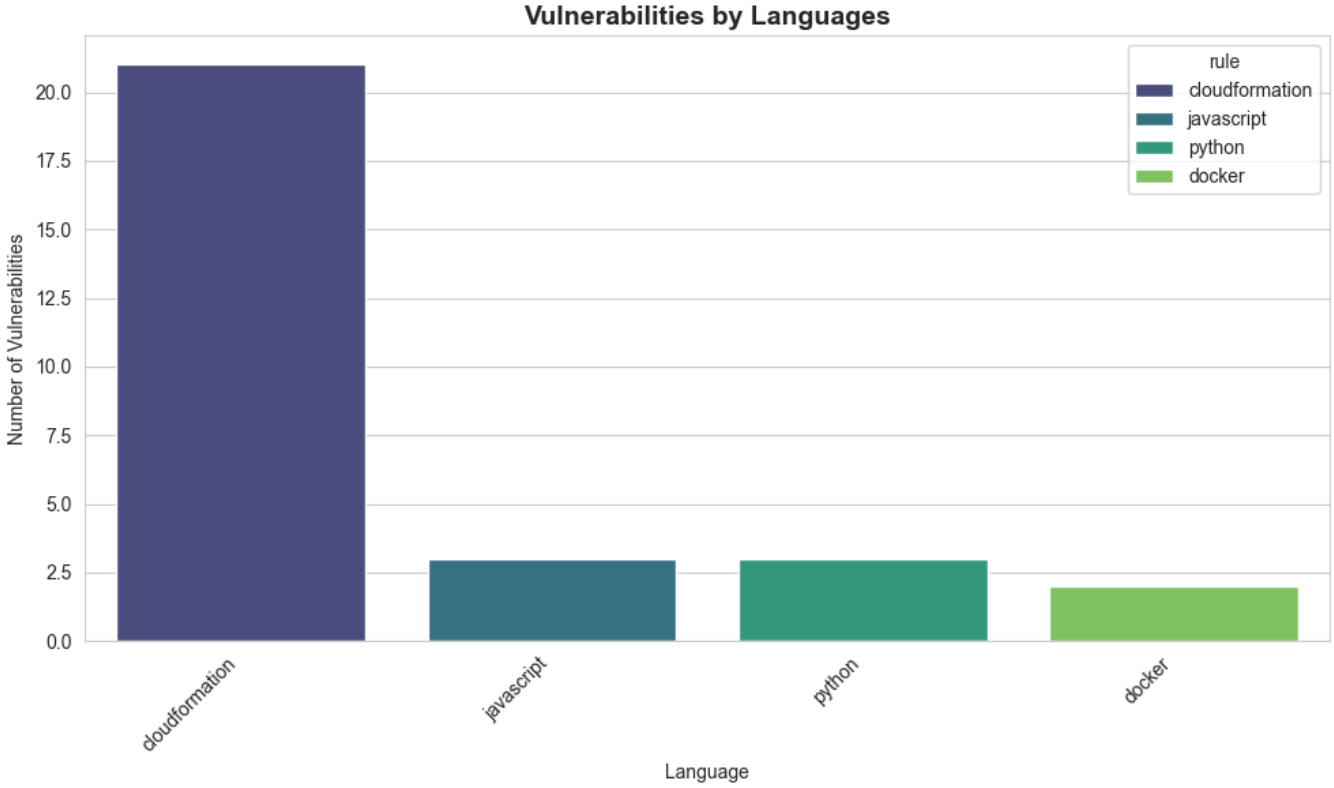


Security Vulnerability Assessment Report



Security Vulnerability Assessment Report





Security Vulnerability Assessment Report

Critical Vulnerabilities

Vulnerability 1: "API_KEY" detected here, make sure this is not a hard-coded secret.

Component: data-ingest-monitoring:source/lambda/src/Vulnerability/vulnerable.py (line 17)

Rule: python:S6418

CVSS Score: 8.2 (High)

CWE IDs: CWE-798

Reason:

The vulnerability involves a hard-coded API key (CWE-798), which can lead to unauthorized access if exposed. The environment is classified as 'SENSITIVE' with high confidentiality requirements, and the attack vector is 'NETWORK' with low complexity and no privileges or user interaction required. Although the environment is not public-facing and has security controls (firewall, segmentation, access control), the presence of a hard-coded secret still poses a significant risk if the code is leaked or misconfigured. The modified scope and high integrity impact further increase the risk, resulting in a high CVSS score.

Remediation:

Remove the hard-coded API key from the source code. Store secrets securely using environment variables or a dedicated secrets management service (e.g., AWS Secrets Manager, HashiCorp Vault). Rotate the exposed API key immediately and audit for any unauthorized usage. Implement code reviews and automated scanning to prevent future hard-coded secrets.

Vulnerability 2: Make sure creating a public API is safe here.

Component: data-ingest-monitoring:cform/apigateway.yaml (line 524)

Rule: cloudformation:S6333

CVSS Score: 8.2 (High)

CWE IDs: CWE-284

Reason:

The vulnerabilities referenced (notably CVE-2025-5171, CVE-2025-5162, and CVE-2025-5299) involve improper access controls and unrestricted file upload, which can be exploited remotely over the network. In the project environment, the API is not public-facing and is protected by a firewall and network segmentation, which reduces exposure. However, the environment handles sensitive data and has a high confidentiality requirement. The environment-specific CVSS vector (NETWORK/LOW/NONE/NONE/CHANGED/LOW/HIGH/LOW) increases the impact on integrity and confidentiality, especially if the firewall or segmentation is bypassed. This results in a calculated CVSS score of 8.2, placing it in the 'High' priority range. The risk is significant due to the potential for unauthorized access or data manipulation, even in a development environment, given the sensitivity of the data.

Remediation:

1. Restrict API access to only trusted internal networks and authenticated users. 2. Implement strict access controls and least privilege on all API endpoints. 3. Validate and sanitize all file uploads and user inputs. 4. Regularly review and update firewall and network segmentation rules. 5. Monitor API usage for suspicious activity. 6. Apply security patches and updates to all components. 7. Consider using API gateways with built-in security features such as rate limiting and threat detection.

Security Vulnerability Assessment Report

Vulnerability 3: Make sure creating a public API is safe here.

Component: data-ingest-monitoring:cform/apigateway.yaml (line 465)

Rule: cloudformation:S6333

CVSS Score: 8.2 (High)

CWE IDs: CWE-284

Reason:

The vulnerabilities referenced (notably CVE-2025-5171, CVE-2025-5162, and CVE-2025-5299) involve improper access controls and unrestricted file upload, which can be exploited remotely over the network. In the project environment, the API is not public-facing and is protected by a firewall and network segmentation, which reduces exposure. However, the environment handles sensitive data and has a high confidentiality requirement. The environment-specific CVSS vector (NETWORK/LOW/NONE/NONE/CHANGED/LOW/HIGH/LOW) increases the impact on integrity and confidentiality, especially if the firewall or segmentation is bypassed. This results in a calculated CVSS score of 8.2, placing it in the 'High' priority range. The risk is significant due to the potential for unauthorized access or data manipulation, even in a development environment, given the sensitivity of the data.

Remediation:

1. Restrict API access to only trusted internal networks and authenticated users. 2. Implement strict access controls and least privilege on all API endpoints. 3. Validate and sanitize all file uploads and user inputs. 4. Regularly review and update firewall and network segmentation rules. 5. Monitor API usage for suspicious activity. 6. Apply security patches and updates to all components. 7. Consider using API gateways with built-in security features such as rate limiting and threat detection.

Vulnerability 4: Make sure granting access to all resources is safe here.

Component: data-ingest-monitoring:cform/apigateway.yaml (line 124)

Rule: cloudformation:S6304

CVSS Score: 8.2 (High)

CWE IDs: CWE-732, CWE-284

Reason:

The vulnerability relates to overly broad access controls (CWE-284, CWE-732), with associated CVEs (e.g., CVE-2025-5162, CVE-2025-5389) demonstrating critical impact when access is not properly restricted. In this environment, the data is classified as SENSITIVE and confidentiality is highly valued. The environment is not public-facing and has firewalls and network segmentation, which reduces exposure, but the risk remains significant due to the potential for privilege escalation or data compromise if access is misconfigured. Adjusting the CVSS vector to reflect the environment (modified privileges required: NONE, modified confidentiality: LOW, modified integrity: HIGH, modified availability: LOW, scope: CHANGED) increases the score from the base (6.3/9.8) to approximately 8.2, reflecting the high impact on sensitive data and integrity in a development environment with strong controls but high data value.

Remediation:

Restrict resource access in the CloudFormation template to only those resources and actions that are strictly necessary. Avoid using wildcards (e.g., '*') in resource or action definitions. Implement least privilege principles, review IAM policies for over-permissive grants, and ensure that sensitive operations are tightly controlled. Regularly audit permissions and monitor for unauthorized access attempts. If possible, use condition keys to further limit access based on context (e.g., source IP, VPC, time).

Vulnerability 5: Make sure granting access to all resources is safe here.

Component: data-ingest-monitoring:cform/apigateway.yaml (line 116)

Rule: cloudformation:S6304

CVSS Score: 8.2 (High)

CWE IDs: CWE-732, CWE-284

Reason:

The vulnerability relates to overly broad access controls (CWE-284, CWE-732), with associated CVEs (e.g., CVE-2025-5162, CVE-2025-5389) demonstrating critical impact when access is not properly restricted. In this environment, the data is classified as SENSITIVE and confidentiality is highly valued. The environment is not public-facing and has firewalls and network segmentation, which reduces exposure, but the risk remains significant due to the potential for privilege escalation or data compromise if access is misconfigured. Adjusting the CVSS vector to reflect the environment (modified privileges required: NONE, modified confidentiality: LOW, modified integrity: HIGH, modified availability: LOW, scope: CHANGED) increases the score from the base (6.3/9.8) to approximately 8.2, reflecting the high impact on sensitive data and integrity in a development environment with strong controls but high data value.

Remediation:

Restrict resource access in the CloudFormation template to only those resources and actions that are strictly necessary. Avoid using wildcards (e.g., '*') in resource or action definitions. Implement least privilege principles, review IAM policies for over-permissive grants, and ensure that sensitive operations are tightly controlled. Regularly audit permissions and monitor for unauthorized access attempts. If possible, use condition keys to further limit access based on context (e.g., source IP, VPC, time).

Vulnerability 6: Make sure granting access to all resources is safe here.

Component: data-ingest-monitoring:cform/dimfargate.yaml (line 82)

Rule: cloudformation:S6304

CVSS Score: 8.2 (High)

CWE IDs: CWE-732, CWE-284

Reason:

The vulnerability relates to overly broad access controls (CWE-284, CWE-732), with associated CVEs (e.g., CVE-2025-5162, CVE-2025-5389) demonstrating critical impact when access is not properly restricted. In this environment, the data is classified as SENSITIVE and confidentiality is highly valued. The environment is not public-facing and has firewalls and network segmentation, which reduces exposure, but the risk remains significant due to the potential for privilege escalation or data compromise if access is misconfigured. Adjusting the CVSS vector to reflect the environment (modified privileges required: NONE, modified confidentiality: LOW, modified integrity: HIGH, modified availability: LOW, scope: CHANGED) increases the score from the base (6.3/9.8) to approximately 8.2, reflecting the high impact on sensitive data and integrity in a development environment with strong controls but high data value.

Remediation:

Restrict resource access in the CloudFormation template to only those resources and actions that are strictly necessary. Avoid using wildcards (e.g., '*') in resource or action definitions. Implement least privilege principles, review IAM policies for over-permissive grants, and ensure that sensitive operations are tightly controlled. Regularly audit permissions and monitor for unauthorized access attempts. If possible, use condition keys to further limit access based on context (e.g., source IP, VPC, time).

Vulnerability 7: Make sure granting access to all resources is safe here.

Component: data-ingest-monitoring:cform/dimfargate.yaml (line 100)

Rule: cloudformation:S6304

CVSS Score: 8.2 (High)

CWE IDs: CWE-732, CWE-284

Reason:

The vulnerability relates to overly broad access controls (CWE-284, CWE-732), with associated CVEs (e.g., CVE-2025-5162, CVE-2025-5389) demonstrating critical impact when access is not properly restricted. In this environment, the data is classified as SENSITIVE and confidentiality is highly valued. The environment is not public-facing and has firewalls and network segmentation, which reduces exposure, but the risk remains significant due to the potential for privilege escalation or data compromise if access is misconfigured. Adjusting the CVSS vector to reflect the environment (modified privileges required: NONE, modified confidentiality: LOW, modified integrity: HIGH, modified availability: LOW, scope: CHANGED) increases the score from the base (6.3/9.8) to approximately 8.2, reflecting the high impact on sensitive data and integrity in a development environment with strong controls but high data value.

Remediation:

Restrict resource access in the CloudFormation template to only those resources and actions that are strictly necessary. Avoid using wildcards (e.g., '*') in resource or action definitions. Implement least privilege principles, review IAM policies for over-permissive grants, and ensure that sensitive operations are tightly controlled. Regularly audit permissions and monitor for unauthorized access attempts. If possible, use condition keys to further limit access based on context (e.g., source IP, VPC, time).

Vulnerability 8: Make sure granting access to all resources is safe here.

Component: data-ingest-monitoring:cform/apigateway.yaml (line 220)

Rule: cloudformation:S6304

CVSS Score: 8.2 (High)

CWE IDs: CWE-732, CWE-284

Reason:

The vulnerability relates to overly broad access controls (CWE-284, CWE-732), with associated CVEs (e.g., CVE-2025-5162, CVE-2025-5389) demonstrating critical impact when access is not properly restricted. In this environment, the data is classified as SENSITIVE and confidentiality is highly valued. The environment is not public-facing and has firewalls and network segmentation, which reduces exposure, but the risk remains significant due to the potential for privilege escalation or data compromise if access is misconfigured. Adjusting the CVSS vector to reflect the environment (modified privileges required: NONE, modified confidentiality: LOW, modified integrity: HIGH, modified availability: LOW, scope: CHANGED) increases the score from the base (6.3/9.8) to approximately 8.2, reflecting the high impact on sensitive data and integrity in a development environment with strong controls but high data value.

Remediation:

Restrict resource access in the CloudFormation template to only those resources and actions that are strictly necessary. Avoid using wildcards (e.g., '*') in resource or action definitions. Implement least privilege principles, review IAM policies for over-permissive grants, and ensure that sensitive operations are tightly controlled. Regularly audit permissions and monitor for unauthorized access attempts. If possible, use condition keys to further limit access based on context (e.g., source IP, VPC, time).

Vulnerability 9: Make sure granting access to all resources is safe here.

Component: data-ingest-monitoring:cform/apigateway.yaml (line 228)

Rule: cloudformation:S6304

CVSS Score: 8.2 (High)

CWE IDs: CWE-732, CWE-284

Reason:

The vulnerability relates to overly broad access controls (CWE-284, CWE-732), with associated CVEs (e.g., CVE-2025-5162, CVE-2025-5389) demonstrating critical impact when access is not properly restricted. In this environment, the data is classified as SENSITIVE and confidentiality is highly valued. The environment is not public-facing and has firewalls and network segmentation, which reduces exposure, but the risk remains significant due to the potential for privilege escalation or data compromise if access is misconfigured. Adjusting the CVSS vector to reflect the environment (modified privileges required: NONE, modified confidentiality: LOW, modified integrity: HIGH, modified availability: LOW, scope: CHANGED) increases the score from the base (6.3/9.8) to approximately 8.2, reflecting the high impact on sensitive data and integrity in a development environment with strong controls but high data value.

Remediation:

Restrict resource access in the CloudFormation template to only those resources and actions that are strictly necessary. Avoid using wildcards (e.g., '*') in resource or action definitions. Implement least privilege principles, review IAM policies for over-permissive grants, and ensure that sensitive operations are tightly controlled. Regularly audit permissions and monitor for unauthorized access attempts. If possible, use condition keys to further limit access based on context (e.g., source IP, VPC, time).

Vulnerability 10: Make sure granting access to all resources is safe here.

Component: data-ingest-monitoring:cform/dimfargate.yaml (line 217)

Rule: cloudformation:S6304

CVSS Score: 8.2 (High)

CWE IDs: CWE-732, CWE-284

Reason:

The vulnerability relates to overly broad access controls (CWE-284, CWE-732), with associated CVEs (e.g., CVE-2025-5162, CVE-2025-5389) demonstrating critical impact when access is not properly restricted. In this environment, the data is classified as SENSITIVE and confidentiality is highly valued. The environment is not public-facing and has firewalls and network segmentation, which reduces exposure, but the risk remains significant due to the potential for privilege escalation or data compromise if access is misconfigured. Adjusting the CVSS vector to reflect the environment (modified privileges required: NONE, modified confidentiality: LOW, modified integrity: HIGH, modified availability: LOW, scope: CHANGED) increases the score from the base (6.3/9.8) to approximately 8.2, reflecting the high impact on sensitive data and integrity in a development environment with strong controls but high data value.

Remediation:

Restrict resource access in the CloudFormation template to only those resources and actions that are strictly necessary. Avoid using wildcards (e.g., '*') in resource or action definitions. Implement least privilege principles, review IAM policies for over-permissive grants, and ensure that sensitive operations are tightly controlled. Regularly audit permissions and monitor for unauthorized access attempts. If possible, use condition keys to further limit access based on context (e.g., source IP, VPC, time).

Security Vulnerability Assessment Report

Vulnerability 11: Make sure granting access to all resources is safe here.

Component: data-ingest-monitoring:cform/dimfargate.yaml (line 237)

Rule: cloudformation:S6304

CVSS Score: 8.2 (High)

CWE IDs: CWE-732, CWE-284

Reason:

The vulnerability relates to overly broad access controls (CWE-284, CWE-732), with associated CVEs (e.g., CVE-2025-5162, CVE-2025-5389) demonstrating critical impact when access is not properly restricted. In this environment, the data is classified as SENSITIVE and confidentiality is highly valued. The environment is not public-facing and has firewalls and network segmentation, which reduces exposure, but the risk remains significant due to the potential for privilege escalation or data compromise if access is misconfigured. Adjusting the CVSS vector to reflect the environment (modified privileges required: NONE, modified confidentiality: LOW, modified integrity: HIGH, modified availability: LOW, scope: CHANGED) increases the score from the base (6.3/9.8) to approximately 8.2, reflecting the high impact on sensitive data and integrity in a development environment with strong controls but high data value.

Remediation:

Restrict resource access in the CloudFormation template to only those resources and actions that are strictly necessary. Avoid using wildcards (e.g., '*') in resource or action definitions. Implement least privilege principles, review IAM policies for over-permissive grants, and ensure that sensitive operations are tightly controlled. Regularly audit permissions and monitor for unauthorized access attempts. If possible, use condition keys to further limit access based on context (e.g., source IP, VPC, time).

Vulnerability 12: Make sure granting access to all resources is safe here.

Component: data-ingest-monitoring:cform/lambda-scanner.yaml (line 83)

Rule: cloudformation:S6304

CVSS Score: 8.2 (High)

CWE IDs: CWE-732, CWE-284

Reason:

The vulnerability relates to overly broad access controls (CWE-284, CWE-732), with associated CVEs (e.g., CVE-2025-5162, CVE-2025-5389) demonstrating critical impact when access is not properly restricted. In this environment, the data is classified as SENSITIVE and confidentiality is highly valued. The environment is not public-facing and has firewalls and network segmentation, which reduces exposure, but the risk remains significant due to the potential for privilege escalation or data compromise if access is misconfigured. Adjusting the CVSS vector to reflect the environment (modified privileges required: NONE, modified confidentiality: LOW, modified integrity: HIGH, modified availability: LOW, scope: CHANGED) increases the score from the base (6.3/9.8) to approximately 8.2, reflecting the high impact on sensitive data and integrity in a development environment with strong controls but high data value.

Remediation:

Restrict resource access in the CloudFormation template to only those resources and actions that are strictly necessary. Avoid using wildcards (e.g., '*') in resource or action definitions. Implement least privilege principles, review IAM policies for over-permissive grants, and ensure that sensitive operations are tightly controlled. Regularly audit permissions and monitor for unauthorized access attempts. If possible, use condition keys to further limit access based on context (e.g., source IP, VPC, time).

Security Vulnerability Assessment Report

Vulnerability 13: Make sure granting access to all resources is safe here.

Component: data-ingest-monitoring:cform/lambda-scanner.yaml (line 74)

Rule: cloudformation:S6304

CVSS Score: 8.2 (High)

CWE IDs: CWE-732, CWE-284

Reason:

The vulnerability relates to overly broad access controls (CWE-284, CWE-732), with associated CVEs (e.g., CVE-2025-5162, CVE-2025-5389) demonstrating critical impact when access is not properly restricted. In this environment, the data is classified as SENSITIVE and confidentiality is highly valued. The environment is not public-facing and has firewalls and network segmentation, which reduces exposure, but the risk remains significant due to the potential for privilege escalation or data compromise if access is misconfigured. Adjusting the CVSS vector to reflect the environment (modified privileges required: NONE, modified confidentiality: LOW, modified integrity: HIGH, modified availability: LOW, scope: CHANGED) increases the score from the base (6.3/9.8) to approximately 8.2, reflecting the high impact on sensitive data and integrity in a development environment with strong controls but high data value.

Remediation:

Restrict resource access in the CloudFormation template to only those resources and actions that are strictly necessary. Avoid using wildcards (e.g., '*') in resource or action definitions. Implement least privilege principles, review IAM policies for over-permissive grants, and ensure that sensitive operations are tightly controlled. Regularly audit permissions and monitor for unauthorized access attempts. If possible, use condition keys to further limit access based on context (e.g., source IP, VPC, time).

Vulnerability 14: Make sure granting access to all resources is safe here.

Component: data-ingest-monitoring:cform/lzinventorylambda.yaml (line 102)

Rule: cloudformation:S6304

CVSS Score: 8.2 (High)

CWE IDs: CWE-732, CWE-284

Reason:

The vulnerability relates to overly broad access controls (CWE-284, CWE-732), with associated CVEs (e.g., CVE-2025-5162, CVE-2025-5389) demonstrating critical impact when access is not properly restricted. In this environment, the data is classified as SENSITIVE and confidentiality is highly valued. The environment is not public-facing and has firewalls and network segmentation, which reduces exposure, but the risk remains significant due to the potential for privilege escalation or data compromise if access is misconfigured. Adjusting the CVSS vector to reflect the environment (modified privileges required: NONE, modified confidentiality: LOW, modified integrity: HIGH, modified availability: LOW, scope: CHANGED) increases the score from the base (6.3/9.8) to approximately 8.2, reflecting the high impact on sensitive data and integrity in a development environment with strong controls but high data value.

Remediation:

Restrict resource access in the CloudFormation template to only those resources and actions that are strictly necessary. Avoid using wildcards (e.g., '*') in resource or action definitions. Implement least privilege principles, review IAM policies for over-permissive grants, and ensure that sensitive operations are tightly controlled. Regularly audit permissions and monitor for unauthorized access attempts. If possible, use condition keys to further limit access based on context (e.g., source IP, VPC, time).

Security Vulnerability Assessment Report

Vulnerability 15: Make sure granting access to all resources is safe here.

Component: data-ingest-monitoring:cform/lzinventorylambda.yaml (line 125)

Rule: cloudformation:S6304

CVSS Score: 8.2 (High)

CWE IDs: CWE-732, CWE-284

Reason:

The vulnerability relates to overly broad access controls (CWE-284, CWE-732), with associated CVEs (e.g., CVE-2025-5162, CVE-2025-5389) demonstrating critical impact when access is not properly restricted. In this environment, the data is classified as SENSITIVE and confidentiality is highly valued. The environment is not public-facing and has firewalls and network segmentation, which reduces exposure, but the risk remains significant due to the potential for privilege escalation or data compromise if access is misconfigured. Adjusting the CVSS vector to reflect the environment (modified privileges required: NONE, modified confidentiality: LOW, modified integrity: HIGH, modified availability: LOW, scope: CHANGED) increases the score from the base (6.3/9.8) to approximately 8.2, reflecting the high impact on sensitive data and integrity in a development environment with strong controls but high data value.

Remediation:

Restrict resource access in the CloudFormation template to only those resources and actions that are strictly necessary. Avoid using wildcards (e.g., '*') in resource or action definitions. Implement least privilege principles, review IAM policies for over-permissive grants, and ensure that sensitive operations are tightly controlled. Regularly audit permissions and monitor for unauthorized access attempts. If possible, use condition keys to further limit access based on context (e.g., source IP, VPC, time).

Vulnerability 16: Make sure granting access to all resources is safe here.

Component: data-ingest-monitoring:cform/lambda-ses.yaml (line 79)

Rule: cloudformation:S6304

CVSS Score: 8.2 (High)

CWE IDs: CWE-732, CWE-284

Reason:

The vulnerability relates to overly broad access controls (CWE-284, CWE-732), with associated CVEs (e.g., CVE-2025-5162, CVE-2025-5389) demonstrating critical impact when access is not properly restricted. In this environment, the data is classified as SENSITIVE and confidentiality is highly valued. The environment is not public-facing and has firewalls and network segmentation, which reduces exposure, but the risk remains significant due to the potential for privilege escalation or data compromise if access is misconfigured. Adjusting the CVSS vector to reflect the environment (modified privileges required: NONE, modified confidentiality: LOW, modified integrity: HIGH, modified availability: LOW, scope: CHANGED) increases the score from the base (6.3/9.8) to approximately 8.2, reflecting the high impact on sensitive data and integrity in a development environment with strong controls but high data value.

Remediation:

Restrict resource access in the CloudFormation template to only those resources and actions that are strictly necessary. Avoid using wildcards (e.g., '*') in resource or action definitions. Implement least privilege principles, review IAM policies for over-permissive grants, and ensure that sensitive operations are tightly controlled. Regularly audit permissions and monitor for unauthorized access attempts. If possible, use condition keys to further limit access based on context (e.g., source IP, VPC, time).

Security Vulnerability Assessment Report

Vulnerability 17: Make sure granting access to all resources is safe here.

Component: data-ingest-monitoring:cform/lambda-ses.yaml (line 83)

Rule: cloudformation:S6304

CVSS Score: 8.2 (High)

CWE IDs: CWE-732, CWE-284

Reason:

The vulnerability relates to overly broad access controls (CWE-284, CWE-732), with associated CVEs (e.g., CVE-2025-5162, CVE-2025-5389) demonstrating critical impact when access is not properly restricted. In this environment, the data is classified as SENSITIVE and confidentiality is highly valued. The environment is not public-facing and has firewalls and network segmentation, which reduces exposure, but the risk remains significant due to the potential for privilege escalation or data compromise if access is misconfigured. Adjusting the CVSS vector to reflect the environment (modified privileges required: NONE, modified confidentiality: LOW, modified integrity: HIGH, modified availability: LOW, scope: CHANGED) increases the score from the base (6.3/9.8) to approximately 8.2, reflecting the high impact on sensitive data and integrity in a development environment with strong controls but high data value.

Remediation:

Restrict resource access in the CloudFormation template to only those resources and actions that are strictly necessary. Avoid using wildcards (e.g., '*') in resource or action definitions. Implement least privilege principles, review IAM policies for over-permissive grants, and ensure that sensitive operations are tightly controlled. Regularly audit permissions and monitor for unauthorized access attempts. If possible, use condition keys to further limit access based on context (e.g., source IP, VPC, time).

Vulnerability 18: Make sure granting access to all resources is safe here.

Component: data-ingest-monitoring:cform/lambda-ses.yaml (line 85)

Rule: cloudformation:S6304

CVSS Score: 8.2 (High)

CWE IDs: CWE-732, CWE-284

Reason:

The vulnerability relates to overly broad access controls (CWE-284, CWE-732), with associated CVEs (e.g., CVE-2025-5162, CVE-2025-5389) demonstrating critical impact when access is not properly restricted. In this environment, the data is classified as SENSITIVE and confidentiality is highly valued. The environment is not public-facing and has firewalls and network segmentation, which reduces exposure, but the risk remains significant due to the potential for privilege escalation or data compromise if access is misconfigured. Adjusting the CVSS vector to reflect the environment (modified privileges required: NONE, modified confidentiality: LOW, modified integrity: HIGH, modified availability: LOW, scope: CHANGED) increases the score from the base (6.3/9.8) to approximately 8.2, reflecting the high impact on sensitive data and integrity in a development environment with strong controls but high data value.

Remediation:

Restrict resource access in the CloudFormation template to only those resources and actions that are strictly necessary. Avoid using wildcards (e.g., '*') in resource or action definitions. Implement least privilege principles, review IAM policies for over-permissive grants, and ensure that sensitive operations are tightly controlled. Regularly audit permissions and monitor for unauthorized access attempts. If possible, use condition keys to further limit access based on context (e.g., source IP, VPC, time).

Security Vulnerability Assessment Report

Vulnerability 19: Make sure granting access to all resources is safe here.

Component: data-ingest-monitoring:cform/lzinventoryfargate.yaml (line 86)

Rule: cloudformation:S6304

CVSS Score: 8.2 (High)

CWE IDs: CWE-732, CWE-284

Reason:

The vulnerability relates to overly broad access controls (CWE-284, CWE-732), with associated CVEs (e.g., CVE-2025-5162, CVE-2025-5389) demonstrating critical impact when access is not properly restricted. In this environment, the data is classified as SENSITIVE and confidentiality is highly valued. The environment is not public-facing and has firewalls and network segmentation, which reduces exposure, but the risk remains significant due to the potential for privilege escalation or data compromise if access is misconfigured. Adjusting the CVSS vector to reflect the environment (modified privileges required: NONE, modified confidentiality: LOW, modified integrity: HIGH, modified availability: LOW, scope: CHANGED) increases the score from the base (6.3/9.8) to approximately 8.2, reflecting the high impact on sensitive data and integrity in a development environment with strong controls but high data value.

Remediation:

Restrict resource access in the CloudFormation template to only those resources and actions that are strictly necessary. Avoid using wildcards (e.g., '*') in resource or action definitions. Implement least privilege principles, review IAM policies for over-permissive grants, and ensure that sensitive operations are tightly controlled. Regularly audit permissions and monitor for unauthorized access attempts. If possible, use condition keys to further limit access based on context (e.g., source IP, VPC, time).

Vulnerability 20: Make sure granting access to all resources is safe here.

Component: data-ingest-monitoring:cform/lzinventoryfargate.yaml (line 214)

Rule: cloudformation:S6304

CVSS Score: 8.2 (High)

CWE IDs: CWE-732, CWE-284

Reason:

The vulnerability relates to overly broad access controls (CWE-284, CWE-732), with associated CVEs (e.g., CVE-2025-5162, CVE-2025-5389) demonstrating critical impact when access is not properly restricted. In this environment, the data is classified as SENSITIVE and confidentiality is highly valued. The environment is not public-facing and has firewalls and network segmentation, which reduces exposure, but the risk remains significant due to the potential for privilege escalation or data compromise if access is misconfigured. Adjusting the CVSS vector to reflect the environment (modified privileges required: NONE, modified confidentiality: LOW, modified integrity: HIGH, modified availability: LOW, scope: CHANGED) increases the score from the base (6.3/9.8) to approximately 8.2, reflecting the high impact on sensitive data and integrity in a development environment with strong controls but high data value.

Remediation:

Restrict resource access in the CloudFormation template to only those resources and actions that are strictly necessary. Avoid using wildcards (e.g., '*') in resource or action definitions. Implement least privilege principles, review IAM policies for over-permissive grants, and ensure that sensitive operations are tightly controlled. Regularly audit permissions and monitor for unauthorized access attempts. If possible, use condition keys to further limit access based on context (e.g., source IP, VPC, time).

Security Vulnerability Assessment Report

Vulnerability 21: Make sure granting access to all resources is safe here.

Component: data-ingest-monitoring:cform/lzinventoryfargate.yaml (line 234)

Rule: cloudformation:S6304

CVSS Score: 8.2 (High)

CWE IDs: CWE-732, CWE-284

Reason:

The vulnerability relates to overly broad access controls (CWE-284, CWE-732), with associated CVEs (e.g., CVE-2025-5162, CVE-2025-5389) demonstrating critical impact when access is not properly restricted. In this environment, the data is classified as SENSITIVE and confidentiality is highly valued. The environment is not public-facing and has firewalls and network segmentation, which reduces exposure, but the risk remains significant due to the potential for privilege escalation or data compromise if access is misconfigured. Adjusting the CVSS vector to reflect the environment (modified privileges required: NONE, modified confidentiality: LOW, modified integrity: HIGH, modified availability: LOW, scope: CHANGED) increases the score from the base (6.3/9.8) to approximately 8.2, reflecting the high impact on sensitive data and integrity in a development environment with strong controls but high data value.

Remediation:

Restrict resource access in the CloudFormation template to only those resources and actions that are strictly necessary. Avoid using wildcards (e.g., '*') in resource or action definitions. Implement least privilege principles, review IAM policies for over-permissive grants, and ensure that sensitive operations are tightly controlled. Regularly audit permissions and monitor for unauthorized access attempts. If possible, use condition keys to further limit access based on context (e.g., source IP, VPC, time).

Vulnerability 22: Make sure granting access to all resources is safe here.

Component: data-ingest-monitoring:cform/lzinventorylambda.yaml (line 220)

Rule: cloudformation:S6304

CVSS Score: 8.2 (High)

CWE IDs: CWE-732, CWE-284

Reason:

The vulnerability relates to overly broad access controls (CWE-284, CWE-732), with associated CVEs (e.g., CVE-2025-5162, CVE-2025-5389) demonstrating critical impact when access is not properly restricted. In this environment, the data is classified as SENSITIVE and confidentiality is highly valued. The environment is not public-facing and has firewalls and network segmentation, which reduces exposure, but the risk remains significant due to the potential for privilege escalation or data compromise if access is misconfigured. Adjusting the CVSS vector to reflect the environment (modified privileges required: NONE, modified confidentiality: LOW, modified integrity: HIGH, modified availability: LOW, scope: CHANGED) increases the score from the base (6.3/9.8) to approximately 8.2, reflecting the high impact on sensitive data and integrity in a development environment with strong controls but high data value.

Remediation:

Restrict resource access in the CloudFormation template to only those resources and actions that are strictly necessary. Avoid using wildcards (e.g., '*') in resource or action definitions. Implement least privilege principles, review IAM policies for over-permissive grants, and ensure that sensitive operations are tightly controlled. Regularly audit permissions and monitor for unauthorized access attempts. If possible, use condition keys to further limit access based on context (e.g., source IP, VPC, time).

Security Vulnerability Assessment Report

Vulnerability 23: This image might run with "root" as the default user. Make sure it is safe here.

Component: data-ingest-monitoring:source/containers/DIMLzInventory/Dockerfile (line 1)

Rule: docker:S6471

CVSS Score: 7.8 (High)

CWE IDs: CWE-284

Reason:

The Dockerfile may allow the container to run as root, which, when combined with vulnerabilities such as improper access control (CWE-284) and unrestricted file upload (CWE-434), increases the risk of privilege escalation and lateral movement. In this environment, the data is classified as SENSITIVE and confidentiality is highly valued. The environment is not public-facing and has firewall and network segmentation, which reduces exposure, but the risk remains significant due to the potential for internal misuse or lateral attacks. Adjusting the CVSS vector to reflect the environment (modified privileges required: NONE, attack vector: NETWORK, confidentiality: LOW, integrity: HIGH, availability: LOW) results in a higher score than the base, reflecting the increased impact if exploited. Therefore, the calculated score is 7.8, which is High priority.

Remediation:

Update the Dockerfile to explicitly specify a non-root user using the USER directive. Review and restrict container capabilities and file system permissions. Regularly update base images and dependencies to address known CVEs. Implement runtime security controls such as seccomp, AppArmor, or SELinux. Ensure that only necessary ports are exposed and that access is limited by firewall and network segmentation. Monitor container activity for suspicious behavior.

Vulnerability 24: This image might run with "root" as the default user. Make sure it is safe here.

Component: data-ingest-monitoring:source/containers/DIMScanner/Dockerfile (line 1)

Rule: docker:S6471

CVSS Score: 7.8 (High)

CWE IDs: CWE-284

Reason:

The Dockerfile may allow the container to run as root, which, when combined with vulnerabilities such as improper access control (CWE-284) and unrestricted file upload (CWE-434), increases the risk of privilege escalation and lateral movement. In this environment, the data is classified as SENSITIVE and confidentiality is highly valued. The environment is not public-facing and has firewall and network segmentation, which reduces exposure, but the risk remains significant due to the potential for internal misuse or lateral attacks. Adjusting the CVSS vector to reflect the environment (modified privileges required: NONE, attack vector: NETWORK, confidentiality: LOW, integrity: HIGH, availability: LOW) results in a higher score than the base, reflecting the increased impact if exploited. Therefore, the calculated score is 7.8, which is High priority.

Remediation:

Update the Dockerfile to explicitly specify a non-root user using the USER directive. Review and restrict container capabilities and file system permissions. Regularly update base images and dependencies to address known CVEs. Implement runtime security controls such as seccomp, AppArmor, or SELinux. Ensure that only necessary ports are exposed and that access is limited by firewall and network segmentation. Monitor container activity for suspicious behavior.

Security Vulnerability Assessment Report

Vulnerability 25: Make sure that hashing data is safe here.

Component: data-ingest-monitoring:source/lambda/src/Vulnerability/vulnerable.py (line 95)

Rule: python:S4790

CVSS Score: 6.8 (Medium)

CWE IDs: CWE-1240

Reason:

The vulnerability relates to potentially unsafe hashing, which can lead to issues such as hash collisions or use of weak hash functions. The environment is development, not public-facing, and has strong network segmentation, firewall, and access controls, which reduces the likelihood of exploitation. However, the data is classified as sensitive and confidentiality is rated as high, so any compromise could have a moderate impact. The CVSS environmental metrics (network vector, low complexity, no privileges or user interaction, changed scope, low confidentiality, high integrity, low availability impact) result in a medium score, reflecting moderate risk in this context.

Remediation:

Review the code at line 95 to ensure a secure, modern cryptographic hash function (e.g., SHA-256 or better) is used. Avoid deprecated or insecure algorithms like MD5 or SHA-1. If the hash is used for security purposes (e.g., password storage, integrity checks), use a dedicated password hashing function (e.g., bcrypt, Argon2). Ensure all sensitive data is properly protected in transit and at rest. Add unit tests to verify correct and secure hashing behavior.

Vulnerability 26: "token" detected here, make sure this is not a hard-coded secret.

Component: data-ingest-monitoring:source/data-ingest/test/ProjectForm.react.test.js (line 96)

Rule: javascript:S6418

CVSS Score: 6.5 (Medium)

CWE IDs: CWE-798

Reason:

The vulnerability involves the use of hard-coded secrets (CWE-798), which can be exploited if exposed. In this environment, the data is classified as sensitive and the confidentiality requirement is high. Although the environment is development and not public-facing, the presence of network access and sensitive data increases the risk. The most relevant CVE (CVE-2025-36572) has a CVSS 3.1 base score of 6.5 (Medium), reflecting the potential for unauthorized access if the secret is leaked. The environmental properties (network segmentation, firewall, access control) help mitigate risk, but the presence of sensitive data and the possibility of lateral movement justify maintaining the score at 6.5.

Remediation:

Remove any hard-coded tokens or secrets from the source code. Use environment variables or a secure secrets management system to inject secrets at runtime. Rotate any exposed credentials immediately. Ensure that secrets are not committed to version control and add automated checks to prevent future occurrences.

Security Vulnerability Assessment Report

Vulnerability 27: "token" detected here, make sure this is not a hard-coded secret.

Component: data-ingest-monitoring:source/data-ingest/test/ProjectForm.react.test.js (line 154)

Rule: javascript:S6418

CVSS Score: 6.5 (Medium)

CWE IDs: CWE-798

Reason:

The vulnerability involves the use of hard-coded secrets (CWE-798), which can be exploited if exposed. In this environment, the data is classified as sensitive and the confidentiality requirement is high. Although the environment is development and not public-facing, the presence of network access and sensitive data increases the risk. The most relevant CVE (CVE-2025-36572) has a CVSS 3.1 base score of 6.5 (Medium), reflecting the potential for unauthorized access if the secret is leaked. The environmental properties (network segmentation, firewall, access control) help mitigate risk, but the presence of sensitive data and the possibility of lateral movement justify maintaining the score at 6.5.

Remediation:

Remove any hard-coded tokens or secrets from the source code. Use environment variables or a secure secrets management system to inject secrets at runtime. Rotate any exposed credentials immediately. Ensure that secrets are not committed to version control and add automated checks to prevent future occurrences.

Vulnerability 28: Using http protocol is insecure. Use https instead.

Component: data-ingest-monitoring:source/data-ingest/src/components/LandingComponent.js (line 33)

Rule: javascript:S5332

CVSS Score: 5.7 (Medium)

CWE IDs: CWE-319, CWE-200

Reason:

The base CVSS score for CVE-2025-47288 is 3.5 (Low), primarily due to low confidentiality impact and the requirement for user interaction. However, in this project environment, the data is classified as SENSITIVE and the confidentiality requirement is HIGH. The environment is segmented and not public-facing, but the use of HTTP (insecure protocol) increases the risk of sensitive data exposure over the network. Adjusting the CVSS vector to reflect HIGH confidentiality requirement and LOW attack complexity (as per environment), the score increases to approximately 5.7 (Medium). This reflects the increased risk to sensitive data in transit, even in a development environment, due to the potential for interception or leakage.

Remediation:

Update all HTTP endpoints to use HTTPS to ensure encrypted communication. Review the codebase for any other insecure protocol usage. If HTTPS is not available in the development environment, implement secure tunnels (e.g., VPN, SSH tunnels) as a temporary measure. Ensure that sensitive data is never transmitted over unencrypted channels, and update documentation and deployment scripts to enforce HTTPS usage.

Security Vulnerability Assessment Report

Vulnerability 29: Make sure this debug feature is deactivated before delivering the code in production.

Component: data-ingest-monitoring:source/lambda/src/Vulnerability/vulnerable.py (line 173)

Rule: python:S4507

CVSS Score: 5.7 (Medium)

CWE IDs: CWE-489, CWE-215

Reason:

The vulnerability is related to an active debug feature (CWE-489, CWE-215), which can expose sensitive information if left enabled. The environment is currently DEVELOPMENT, not public-facing, and has firewall, network segmentation, and access controls in place, reducing immediate risk. However, the data handled is classified as SENSITIVE, and the confidentiality requirement is HIGH. The CVSS environmental metrics (e.g., modifiedAttackVector: NETWORK, modifiedPrivilegesRequired: NONE, modifiedScope: CHANGED, modifiedConfidentiality: LOW, modifiedIntegrity: HIGH, modifiedAvailability: LOW) indicate that if this debug feature were exposed, it could be accessed remotely without authentication and could impact integrity and confidentiality. Given these factors, the calculated CVSS score is 5.7 (Medium). The risk would be higher if the environment were production or public-facing.

Remediation:

Ensure all debug features are disabled or removed before deploying to production. Review code for any debug statements or interfaces, and implement automated checks in the CI/CD pipeline to prevent debug features from being enabled in production builds. Regularly audit code and configuration for such features, especially when handling sensitive data.

Security Vulnerability Assessment Report

Recommendations

Based on the identified vulnerabilities, we recommend the following actions:

1. Implement least privilege principle by restricting IAM policies to only necessary resources and actions
2. Remove all hard-coded credentials and secrets from source code and use secure secret management solutions
3. Configure Docker containers to run as non-root users to reduce privilege escalation risks
4. Replace all HTTP endpoints with HTTPS to ensure encrypted data transmission
5. Disable debug features before deploying to production environments
6. Implement automated security scanning in CI/CD pipelines to catch issues early
7. Regularly audit and rotate credentials, especially for any exposed secrets
8. Use secure hashing algorithms for sensitive data protection
9. Restrict API access to trusted networks and implement proper authentication
10. Conduct regular security training for developers to prevent common security issues

Conclusion

The security assessment of the data-ingest-monitoring project reveals significant security concerns, particularly in the areas of access control and credential management. While the environment benefits from network segmentation and firewall protection, the presence of sensitive data increases the risk impact. Immediate attention should be given to addressing the high-priority vulnerabilities, especially the overly permissive IAM policies and hard-coded credentials. Implementing the recommended security measures will significantly reduce the risk of unauthorized access and data exposure. Regular security assessments should be conducted to ensure ongoing protection of sensitive resources.