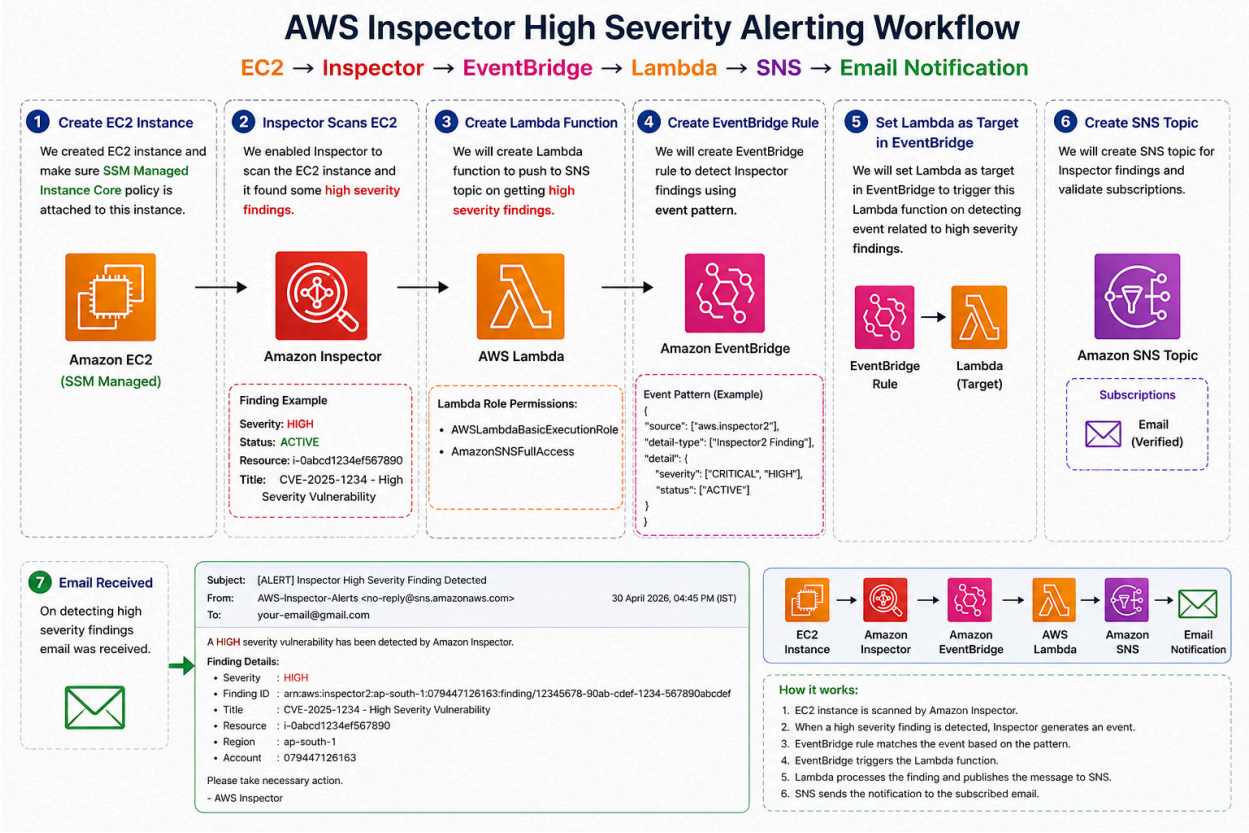
Cloud-Native Vulnerability Detection & Alerting Pipeline

Project Overview:

Designed and implemented an event-driven security monitoring pipeline using Amazon Inspector, Amazon EventBridge, AWS Lambda, and Amazon SNS to automatically detect and notify on high-severity vulnerabilities in EC2 workloads.

The solution continuously scans compute resources, filters critical findings in real time, and triggers alerts without manual intervention—ensuring faster response to security risks.



Tools & Services Used

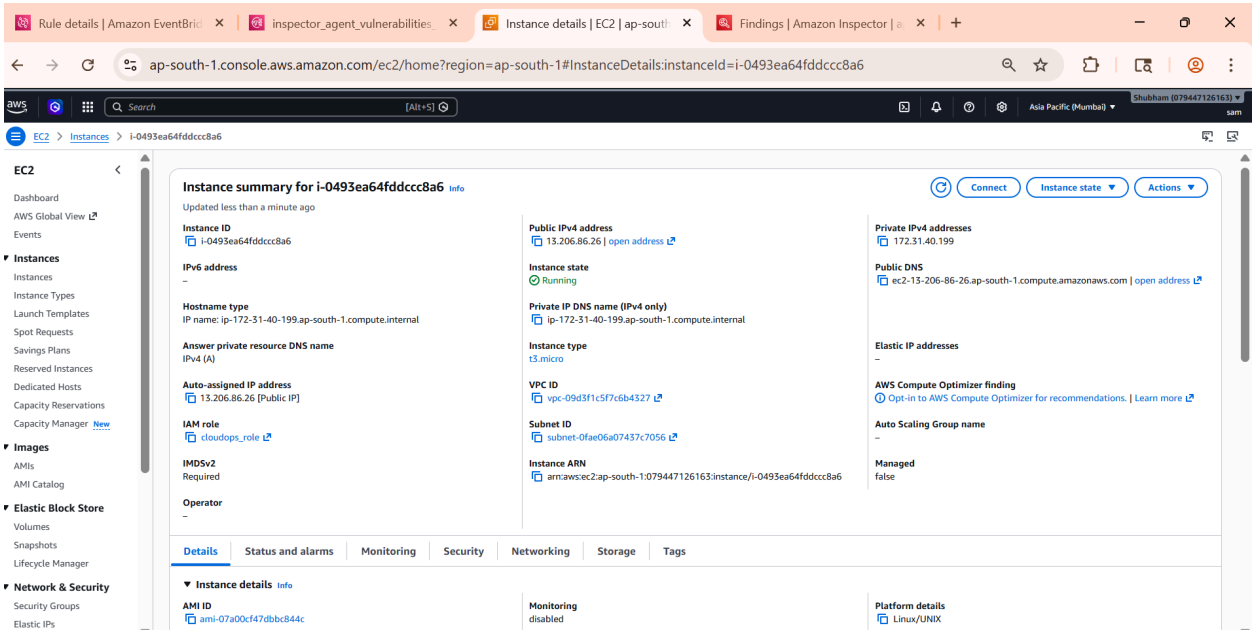
- Amazon EC2
- Amazon Inspector
- Amazon EventBridge
- AWS Lambda

- Amazon SNS
- AWS Systems Manager

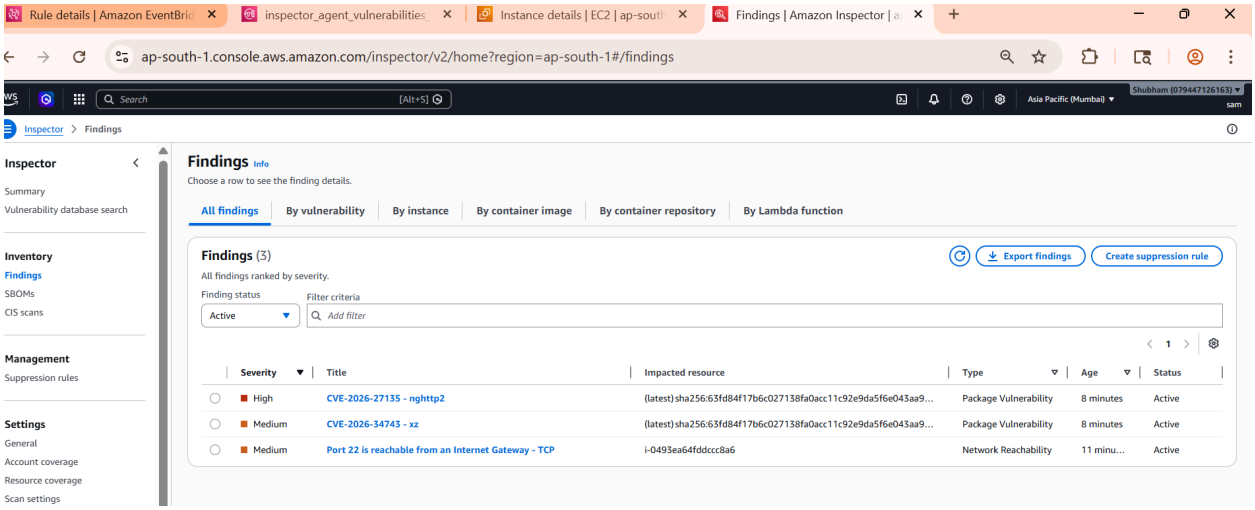
Outcomes / Impact

- ⚡ Reduced vulnerability detection-to-notification time to near real-time
- 🔍 Improved visibility into critical security findings
- 🚫 Eliminated manual monitoring effort
- 📈 Enabled proactive remediation workflows
- 🧩 Built a scalable, event-driven security automation pipeline

Step 1 — EC2 Setup
Created an EC2 instance and attached an IAM role with `AmazonSSMManagedInstanceCore` policy to enable Systems Manager integration and secure management.

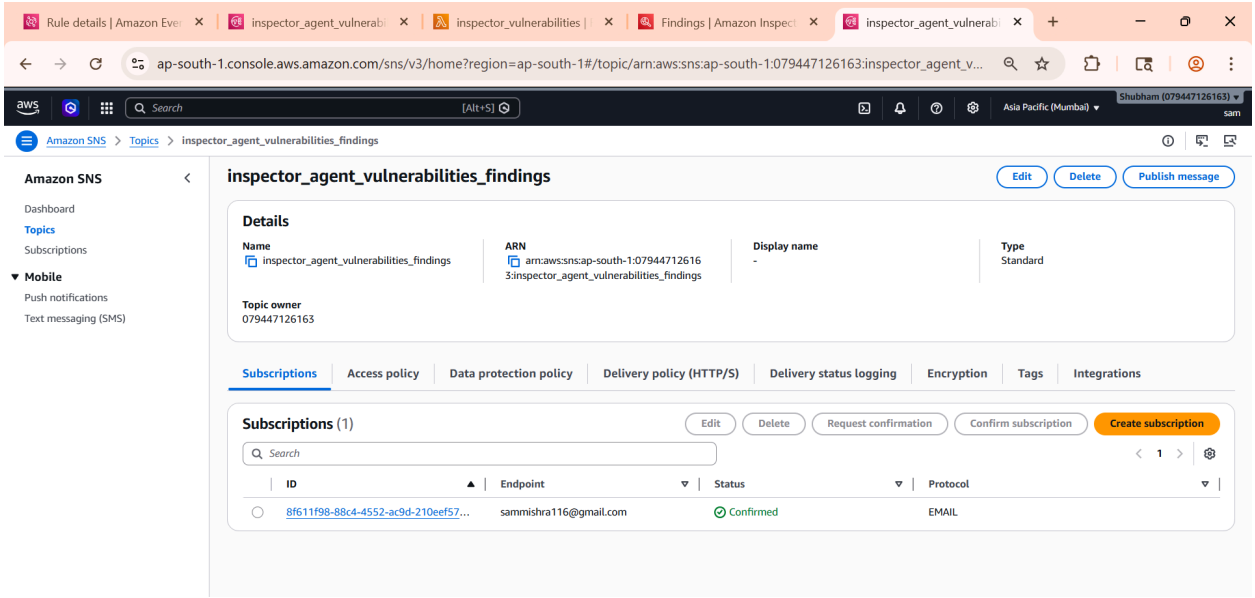


Step 2 — Enable Vulnerability Scanning
Enabled Amazon Inspector to continuously scan the EC2 instance and identify vulnerabilities, including HIGH severity findings.



Step 3 — SNS Topic Configuration (Corrected Order)

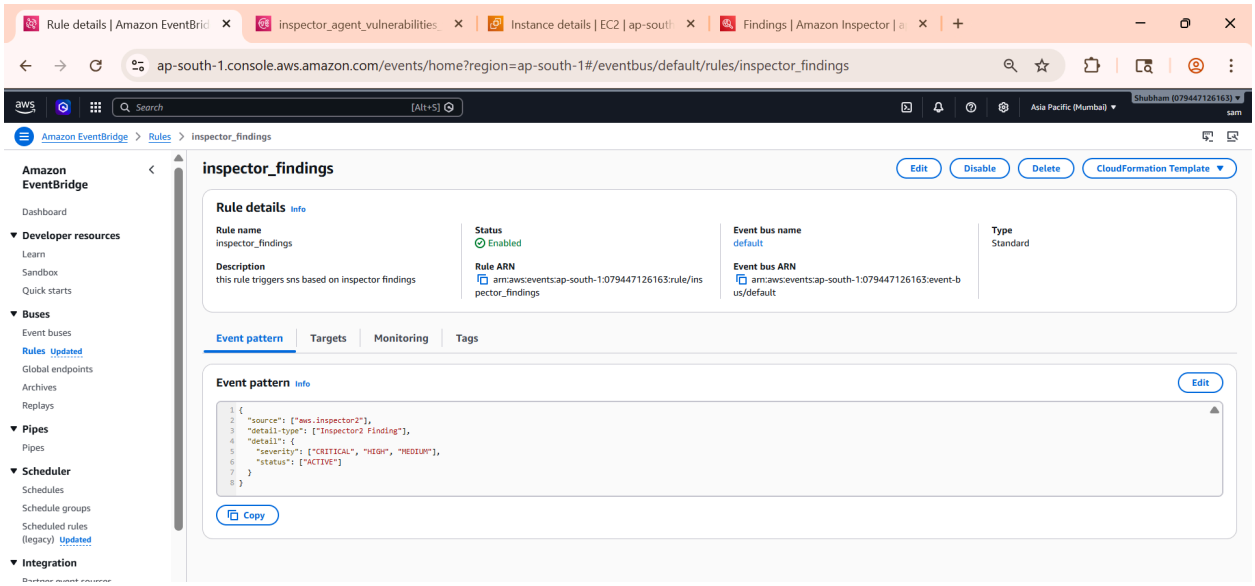
Created an SNS topic for vulnerability alerts and configured email subscriptions. Verified subscription via confirmation email.



Step 4 — EventBridge Rule Creation

Configured an EventBridge rule with an event pattern to capture Inspector findings filtered by:

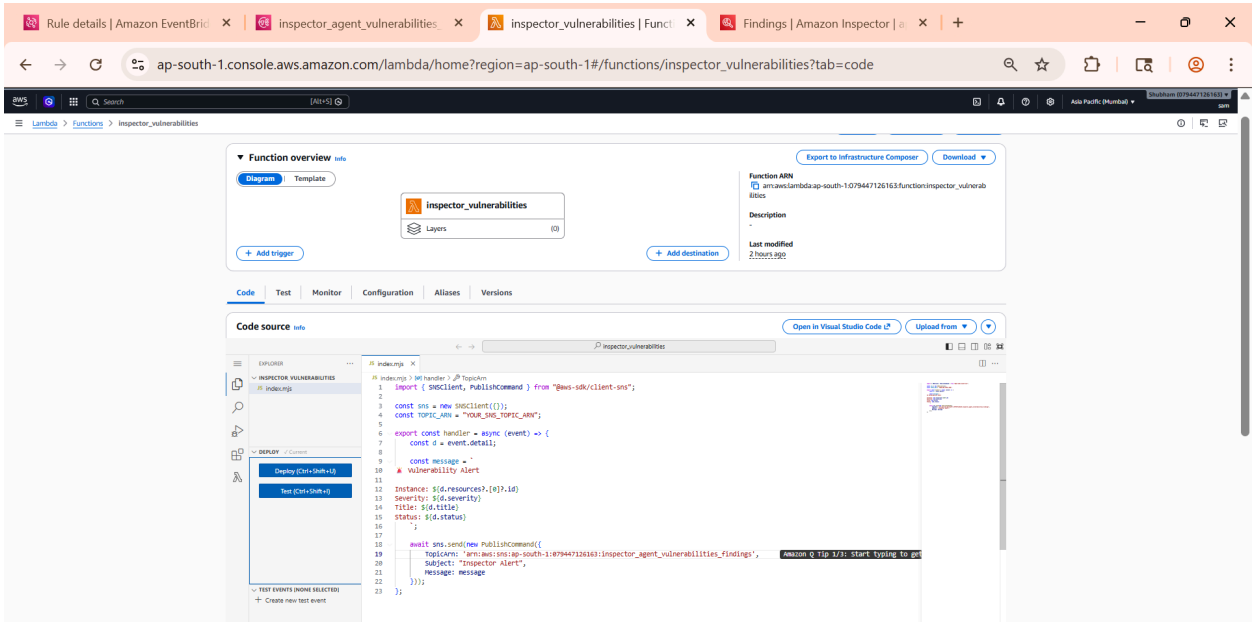
- Severity: HIGH / CRITICAL
- Status: ACTIVE



Step 5 — Lambda Function (Optional Processing Layer)

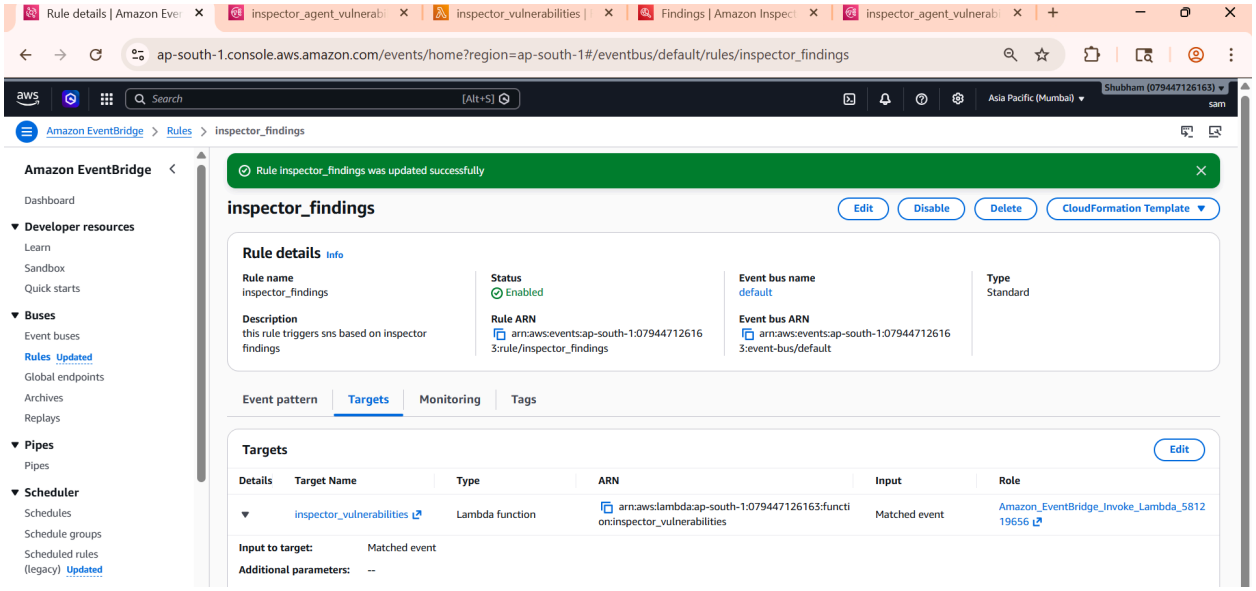
Created a Lambda function to:

- Parse Inspector findings
- Format alert messages
- Forward notifications to SNS



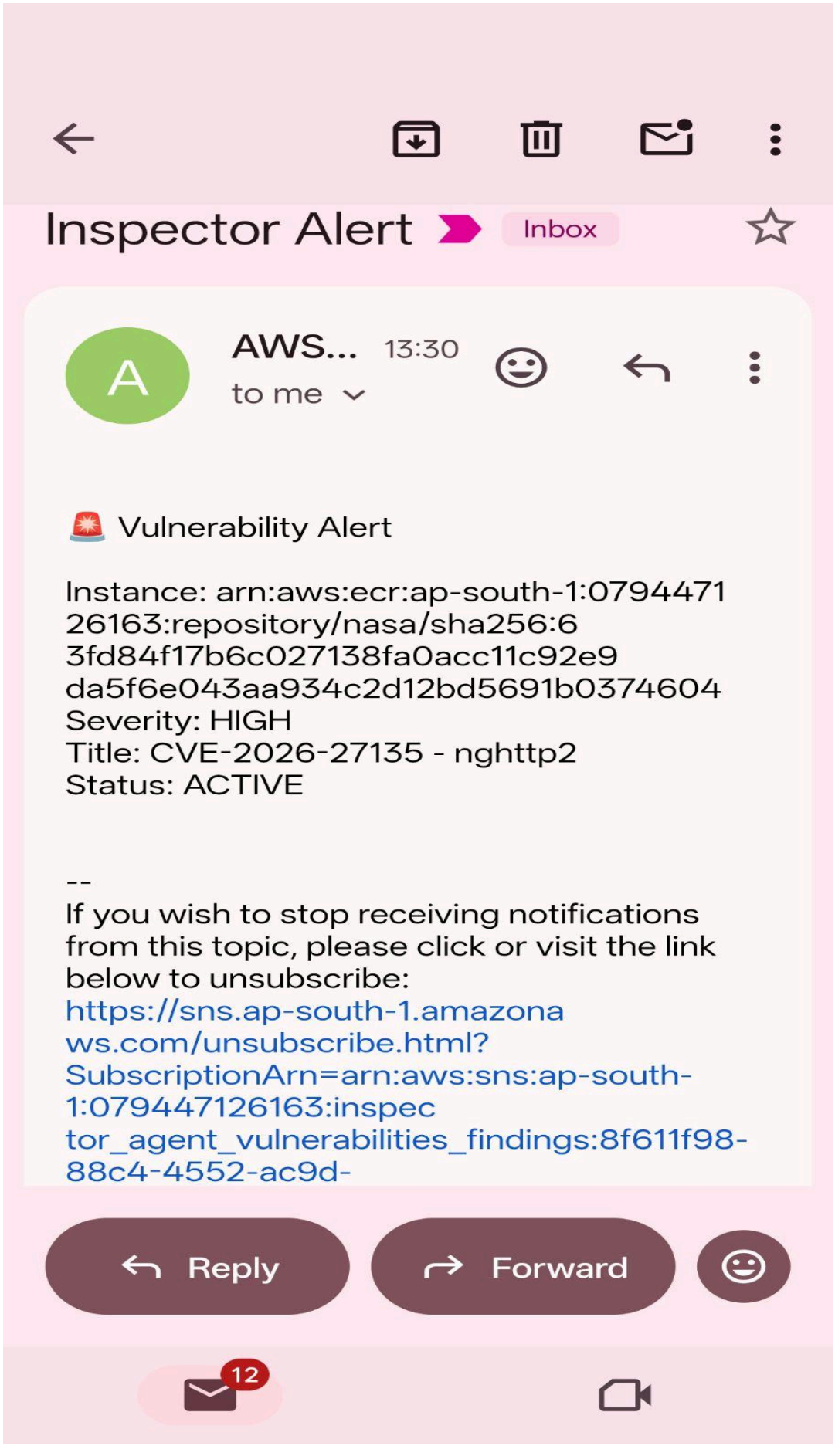
Step 6 — Target Integration

Attached Lambda as the target of the EventBridge rule to trigger processing upon matching Inspector events.



Step 7 — Alert Validation

Triggered high-severity findings and verified that email notifications were successfully received via SNS.


Inspector Alert
Inbox
A
AWS...
13:30
to me
Vulnerability Alert
Instance: arn:aws:ecr:ap-south-1:079447126163:repository/nasa/sha256:63fd84f17b6c027138fa0acc11c92e9da5f6e043aa934c2d12bd5691b0374604
Severity: HIGH
Title: CVE-2026-27135 - nghttp2
Status: ACTIVE
--
If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
https://sns.ap-south-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:ap-south-1:079447126163:inspector_agent_vulnerabilities_findings:8f611f98-88c4-4552-ac9d-
Reply
Forward
12