CONSOLIDATED SECURITY ASSESSMENT REPORT

Amazon ECS Fullstack App (Terraform Demo)

Date: 2026-02-18

Classification: CONFIDENTIAL

Methodology: STRIDE-LM + PASTA + OWASP Risk Rating | CVSS v3.1 | LINDDUN

Table of Contents

I. Executive Summary

Overall Security Posture: CONCERNING

This AWS ECS demo/reference architecture contains significant security gaps that make it unsuitable for production use without substantial hardening. The assessment identified **26 unique findings** across four specialist domains, with two CRITICAL-severity issues enabling full AWS account compromise via the CI/CD pipeline.

Severity	Count	Scoring System
CRITICAL	2	OWASP Risk Rating
HIGH	10	OWASP Risk Rating
MEDIUM	11	OWASP Risk Rating
LOW	3	OWASP Risk Rating
Total	26	

Top 3 Risks

1. Repository-Sourced Buildspec (TM-004, CRITICAL, 25): Any developer with GitHub push access can execute arbitrary commands with near-admin AWS permissions.

2. IAM PassRole Wildcard (TM-003, CRITICAL, 20): Both DevOps and ECS task roles enable privilege escalation to any role in the account.

3. No TLS on ALBs (TM-001, HIGH, 15): All user traffic traverses the internet in plaintext.

Metric	Value
Components Assessed	26
Data Flows Mapped	25+
Trust Boundaries	8
Threat Actors	5
Unique Findings	26

II. System Overview

System Purpose: AWS ECS Fargate-based fullstack web application serving a product catalog, deployed via Terraform. Designed as a demo/reference architecture.

Layer	Technology	Version	Notes
Frontend	Vue.js + Bootstrap-Vue	2.6.11	SPA via Nginx
Backend	Node.js + Express	4.16.4	API + Swagger
Container	AWS Fargate	LATEST	awsvpc mode
Data Store	DynamoDB	PAY_PER_REQUEST	Product catalog
CI/CD	CodePipeline/Build/Deploy	V1	Blue/Green
IaC	Terraform	>= 0.13	AWS ~> 3.38

III. Architecture Diagram

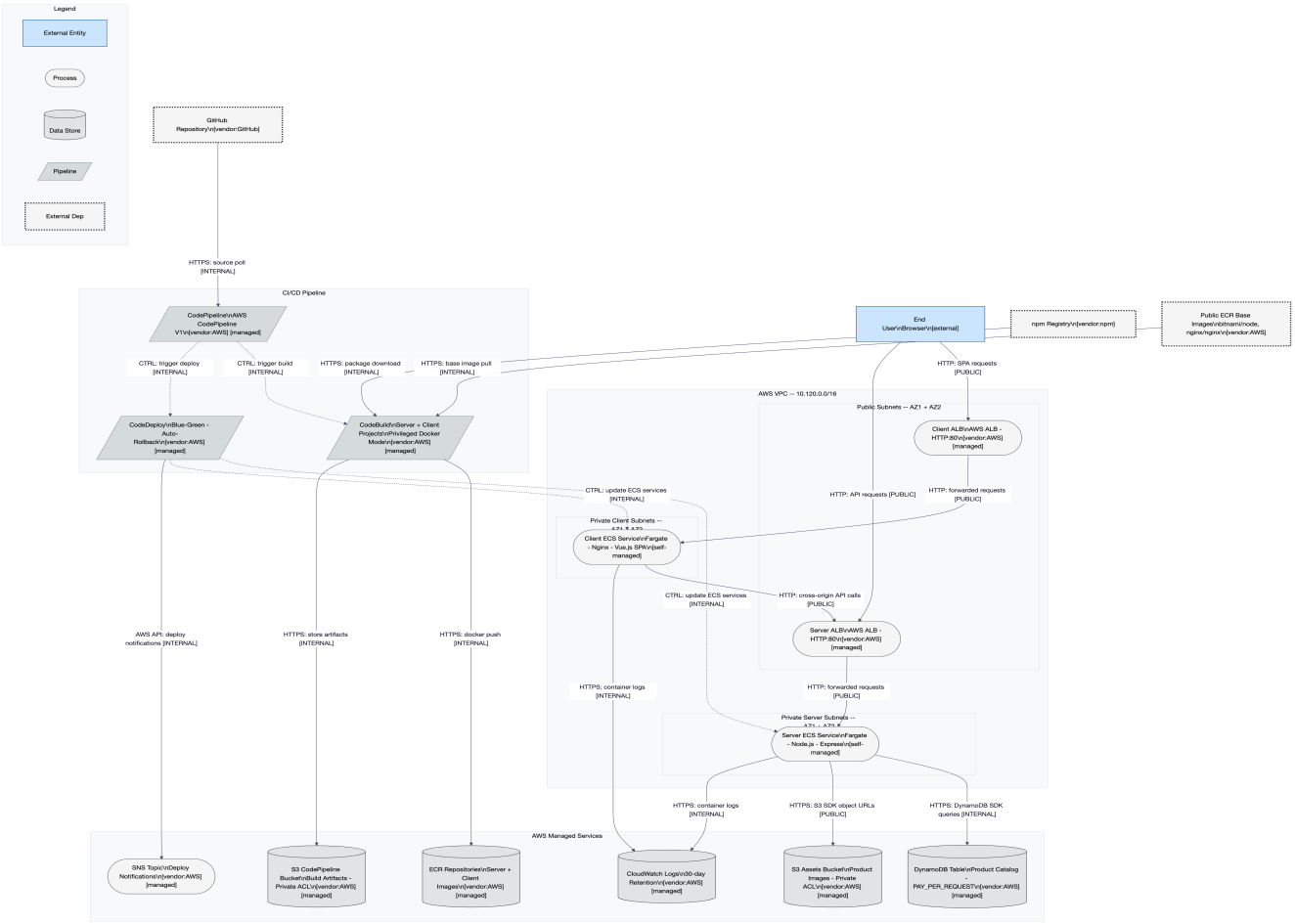

Figure 1: L1 Structural Architecture Diagram

IV. Risk Overlay Diagram

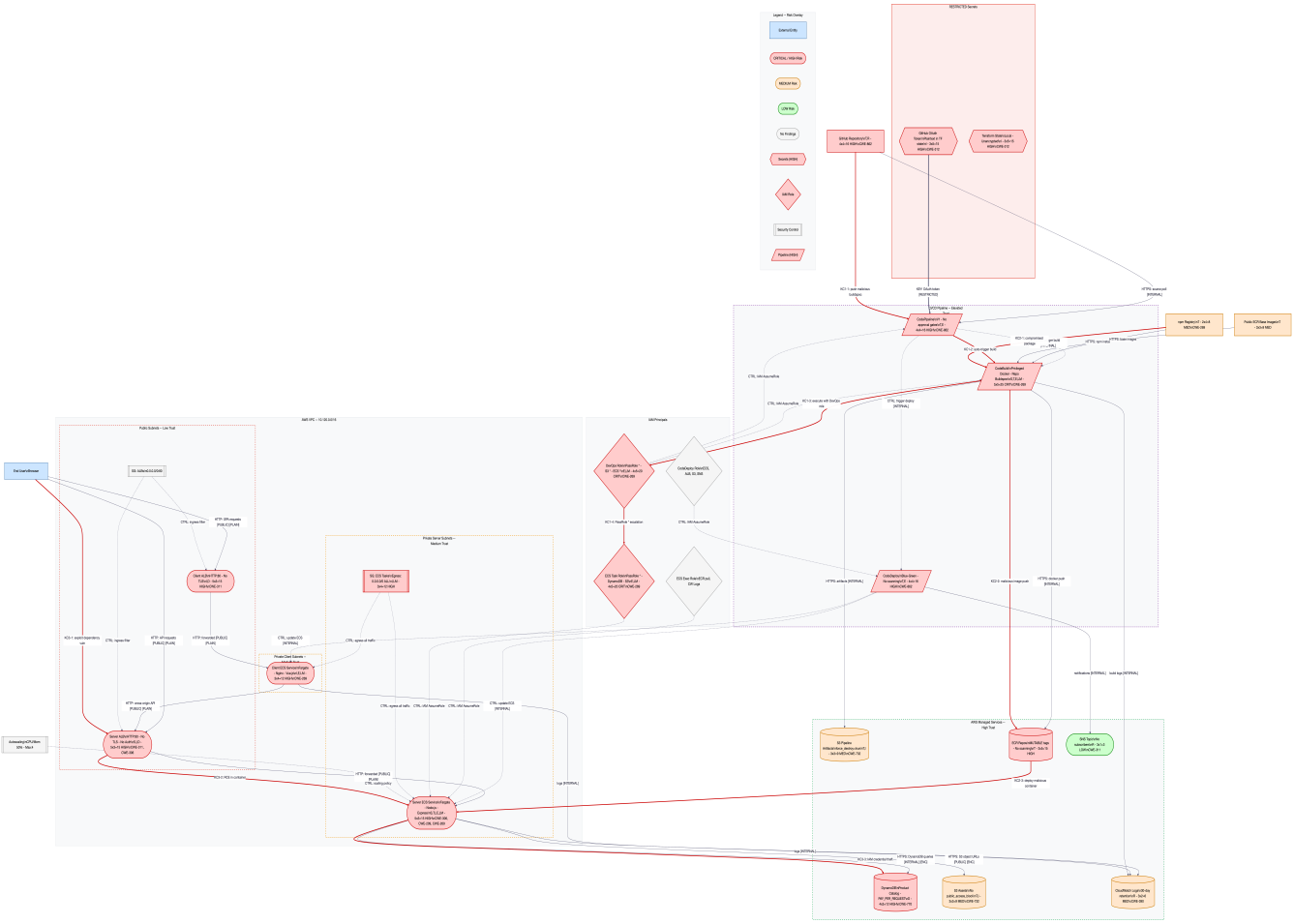

Figure 2: L4 Risk Overlay with Kill Chain Overlays

VII. Findings (Summary)

ID	Severity	Title	Lxl=Score
TM-004	CRITICAL	Repository-Sourced Buildspec + Broad IAM	5x5=25
TM-003	CRITICAL	IAM PassRole Wildcard (*)	4x5=20
TM-023	HIGH	No Branch Protection	4x4=16
TM-013	HIGH	CodeBuild Privileged Docker	4x4=16
TM-014	HIGH	No Pipeline Approval / Scanning	4x4=16
TM-001	HIGH	No TLS/HTTPS on ALBs	5x3=15
TM-002	HIGH	No Authentication/Authorization	5x3=15
TM-005	HIGH	GitHub Token in TF State	3x5=15
TM-006	HIGH	Mutable ECR Tags + Latest	3x5=15
TM-007	HIGH	No WAF or Rate Limiting	4x3=12
TM-022	HIGH	Unrestricted ECS Egress	3x4=12
TM-024	HIGH	No Billing Alarm	4x3=12
TM-009	MEDIUM	S3 Missing Security Controls	3x3=9
TM-011	MEDIUM	No VPC Flow Logs	3x3=9
TM-015	MEDIUM	Outdated Dependencies	3x3=9
TM-017	MEDIUM	Container Hardening Deficiencies	3x3=9
TM-012	MEDIUM	Error Handler Info Leakage	4x2=8
TM-025	MEDIUM	npm install vs npm ci	2x4=8
TM-008	MEDIUM	Unrestricted CORS	3x2=6
TM-018	MEDIUM	Single NAT GW (SPOF)	2x3=6
TM-021	MEDIUM	No Container Insights	3x2=6
TM-026	MEDIUM	No CloudTrail Data Events	3x2=6
TM-016	MEDIUM	Swagger Publicly Exposed	5x1=5
TM-010	LOW	DynamoDB No PITR/CMK	2x2=4
TM-019	LOW	No VPC Endpoints	2x2=4
TM-020	LOW	SNS No Subscribers/Encryption	3x1=3

Total: 26 findings (2 critical, 10 high, 11 medium, 3 low)

VIII. Remediation Roadmap

Wave 1: Quick Wins (1-2 days)

R-001: ECR immutable tags

R-002: S3 public_access_block

R-003: DynamoDB PITR

R-004: npm ci

R-005: Billing alarm

Wave 2: Critical Fixes (1-2 sprints)

R-011: Scope IAM PassRole

R-012: Secure buildspec

R-013: Branch protection

R-014: Pipeline approval

R-015: Enable HTTPS

Wave 3: Hardening (2-4 sprints)

R-020: VPC Flow Logs

R-022: Container hardening

R-024: Pipeline scanning

R-025: Update dependencies

Wave 4: Production Ready

R-028: Implement authentication

R-029: VPC endpoints

R-030: Git SHA image tags

R-031-033: S3/SNS cleanup

X. Compliance Mapping

Framework	Total	Compliant	Partial	Non-Compliant	N/A	Coverage
SOC 2	33	3	6	22	2	9%
ISO 27001	93	5	8	41	39	10%
NIST CSF 2.0	106	4	9	38	55	8%
PCI-DSS v4.0	64	1	3	48	12	2%

XI. Privacy Assessment

10 privacy findings: 2 critical, 3 high, 3 medium, 2 low. Key issues: no TLS, deceptive login form, no privacy notice, developer PII in Swagger.

XII. Positive Observations

- Private subnets with SG segmentation
- Fargate isolation
- Blue/Green deployment with auto-rollback
- Read-only DynamoDB access
- awsvpc network mode
- Infrastructure as Code (Terraform)

XIII. Assumptions & Limitations

Single AWS account. Demo context. No runtime scanning, penetration testing, or Terraform plan execution performed.

XIV. Appendices

A. OWASP bands: CRITICAL (20-25), HIGH (12-19), MEDIUM (6-11), LOW (1-5)

B. See HTML report for complete MITRE/CWE reference tables

C. QA: HIGH count corrected 9->10. 14 duplicates deduplicated. 3 confidence escalations.

D. Glossary: See HTML report for full glossary

E. Re-assess when: auth added, PII handled, new endpoints, production deploy, CI/CD changes