DevSecOps for the Community: Building, Provisioning and Deploying CVE's Infrastructure and Services

MAY 11, 2023
Shane T. Ficorilli
Senior Cybersecurity Engineer
MITRECorp

PITTSBURGH
Agenda

- Who am I?
- What is CVE?
- DevSecOps Culture
- CVE-Services
- New CVE-Website: cve.org
- Future DevSecOps Improvements
- Questions?
Who am I? – Shane T. Ficorilli

• Born and raised in Pittsburgh, PA
• Education:
  • BS in IT/Minor in Computer Science – La Roche College
  • MS in Information Security Policy and Management – Carnegie Mellon University
• Work Experience:
  • 2016-2021: DevSecOps/Software Engineer – Software Engineering Institute
  • 2021-Present: Senior Cyber Security Engineer – MITRECorp
What is CVE?
What is CVE?

- Common Vulnerabilities and Exposures (CVE)
- The mission of the CVE® Program is to uniquely identify, catalog and publish helpful information concerning publicly disclosed cybersecurity vulnerabilities
- There is one CVE Record for each vulnerability in the catalog
- The vulnerabilities are discovered then assigned and published by CVE Numbering Authorities (CNAs) that have partnered with the CVE Program
- Launched to the public in September 1999
- Systems operated by MITRE
What is CVE? – System of Systems

CVE List
Downstream Users

CVE List Bulk Download (JSON 5.0)

CVE Services

CVE ID Reservation Service (IDR)
Record Submission Upload and Service (RSUS)
User Registry

CVE Services Clients/Registered Users

CNAs
Roots
Secretariat

API Access

User Registry Authorization data store

Unregistered/Registered Users

General Users
Researchers
CNAs
JSON 5.0 Web Submission

CVE Program Web Site/CVE Services Program Client

JSON 5.0 CVE List GitHub Download
DevSecOps Culture
DevSecOps Culture

• Development, security and operations teams work closely together
  • Implement new features
  • Track effort/issues
  • Oversee/troubleshoot deployments
  • Alerting/monitoring

• Community Involvement & Feedback– Working Groups
  • Automation Working Group (AWG)
  • Website Working Group (WSWG)
DevSecOps for the Community: Building, Provisioning and Deploying CVE's Infrastructure and Services

CVE-Services
CVE-Services

- A web addressable application for CVE Number Authorities (CNAs)

- Comprises a series of RESTful endpoints/Application Programming Interfaces (APIs) to which CNA “clients” will connect to perform common functions such as:
  - Reserving a CVE ID
  - Submitting/Updating a CVE Record for publication
  - Manage the CVE Services users at your CNA (i.e., create accounts, change password)

- Instantaneous, Automatic response
  - No human intervention, no lag time
CVE-Services

- CVE-Services source code lives on GitHub

- All infrastructure created using AWS CloudFormation Templates stored in MITRE’s internal GitLab

- Five different environments exist in AWS
CVE-Services Environments

DevSecOps for the Community: Building, Provisioning and Deploying CVE's Infrastructure and Services
CVE-Services CI/CD Architecture
CVE-Services CI/CD Components

- GitHub Repository
- GitHub Advanced Security tools:
  - Dependabot scans/alerting
  - CodeQL SAST scans

- AWS
  - Code Pipeline
  - Code Build
  - S3
  - ECR (Elastic Container Registry)
  - ECS (Elastic Container Service: Fargate)
CVE-Services AWS Components

- Elastic Container Service
- Elastic Container Registry
- DocumentDB EC2 (Bastion host to access DocumentDB instance)
  - MITRE vetted Amazon Linux2 AMI
- ALB (Application Load Balancer)
- VPC (private/public subnets)
- IAM (Identity and Access Management)
- Cloud Watch (logs)
- WAF (Web Application Firewall)
DevSecOps for the Community: Building, Provisioning and Deploying CVE's Infrastructure and Services

CVE-Website (cve.org)
- Old Website hosted on prem by MITRE
- cve.mitre.org
• New Website hosted by MITRE owned AWS infrastructure

• cve.org
CVE-Website

- Static website using CVE-Services API to dynamically generate content
- CVE-Website source code lives on GitHub
- All infrastructure created using AWS CloudFormation Templates stored in MITRE’s internal GitLab
- Four different environments exist in AWS (separate account)
CVE-Website Environments
CVE-Website CI/CD Architecture
CVE-Website CI/CD Components

- GitHub Repository
- GitHub Advanced Security tools:
  - Dependabot scans/alerting
  - CodeQL SAST scans

- AWS
  - Code Build
  - Code Pipeline
  - S3
  - CloudFront
CVE-Website AWS Components

- S3
- Cloud Front
- Cloud Watch
- Lambda
- API Gateway
- Route53
- VPC
- IAM
- SES (Simple Email Service)
- WAF
Future DevSecOps Improvements
Future DevSecOps Improvements

- Dynamic Application Security Testing (DAST)
- Currently no automated DAST solutions in place
  - Burp Suite
  - OWASP Zap
- Improved Monitoring Strategy
  - Additional AWS resource monitoring
  - MITRE internal security monitoring
  - DevSecOps metrics
Questions?
References

- https://github.com/CVEProject/cve-services
- https://www.cve.org/AllResources/CveServices
- https://github.com/CVEProject/cve-website
- https://www.cve.org/About/Overview
Contact Information

Shane T. Ficorilli
Senior Cyber Security Engineer

Email: sficorilli@mitre.org