# **Issue Document**

## **Title: Publicly Exposed Serverless Function with Text4Shell Vulnerability (CVE-2022-42889) Leading to PII Exposure**

* **Date:** [Insert Date]
* **Author:** [Your Name/Team]
* **Status:** Resolved

## **Affected Systems/Components**

* **Serverless Function:** xl-excel Macro-dev (Lambda)
* **AWS Account:** Associated with ignaite-license and terraform-fuse-dts.us-east-1.appfire.app
* **IAM Role:** Lambda ExRole

### **Sensitive Resources**

* **S3 Bucket:** ignaite-license (PII/Email data)
* **S3 Bucket:** terraform-fuse-dts.us-east-1.appfire.app (Infrastructure state)

## **1. Issue Description**

### **Overview**

* The Lambda function **xl-excel Macro-dev** was exposed via two **public endpoints** and vulnerable to **CVE-2022-42889 (Text4Shell)** in the **Apache Commons Text library (v1.8)**.
* Attackers could exploit this to **execute arbitrary code**, assume the **overprivileged Lambda ExRole**, and access **sensitive PII/Email data**.

### **Affected Resources**

* **Exposed Endpoints:**
  + https://apixl-dev.dts-bobswift.appfire.app:443/api/1.0/excel
  + https://0z5jyn4ez6.execute-api.us-east-1.amazonaws.com:443/prod/1.0/excel
* **Vulnerable Library:** Apache Commons Text (**v1.8**)
* **AWS Resources at Risk:**
  + **ignaite-license** – [Link to S3 Bucket]
  + **terraform-fuse-dts.us-east-1.appfire.app** – [Link to Terraform State]

### **Impact**

* **Data Breach:** Unauthorized access to **PII/Email data** in ignaite-license.
* **Infrastructure Risk:** Potential tampering with **Terraform state files** in terraform-fuse-dts.us-east-1.appfire.app.
* **Regulatory Penalties:** Potential violations of **GDPR, CCPA, or HIPAA**.

## **2. Issue Resolution**

### **Issue 1: Public Exposure of Serverless Endpoints**

**Root Cause:**

* Publicly accessible **API Gateway endpoints** with **no authentication**.

**Fixes Implemented:**

* Enabled **AWS API Gateway resource policies** to restrict access to **trusted IPs**.
* Implemented **IAM authentication** for **API Gateway**.

**Validation:**

* **Penetration testing** confirmed restricted access.
* **AWS CloudTrail logs** reviewed for unauthorized requests.

### **Issue 2: CVE-2022-42889 (Text4Shell) Exploitation**

**Root Cause:**

* Outdated **Apache Commons Text library (v1.8)**.

**Fixes Implemented:**

* Upgraded library to patched version **1.10.0**.
* Scanned dependencies using **AWS Lambda Layer versioning**.

**Validation:**

* **Vulnerability scan** (e.g., Trivy) confirmed no **CVE-2022-42889** exposure.
* **Exploit simulation** using **Metasploit** blocked post-patch.

### **Issue 3: Overprivileged Lambda ExRole**

**Root Cause:**

* Excessive permissions (e.g., **s3:Get\***, **terraform:**\*) granted to **Lambda ExRole**.

**Fixes Implemented:**

* **Revised IAM policies** to enforce **least privilege** (e.g., revoked s3:GetObject on sensitive buckets).
* **Encrypted S3 buckets** using **AWS KMS**.

**Validation:**

* **AWS CLI test:** aws s3 ls s3://ignaite-license **denied** for unauthorized roles.
* **IAM Access Analyzer report** confirmed **reduced permissions**.

## **3. Prevention/Follow-Up Actions**

### **API Security**

* Use **AWS WAF** to block **malicious payloads** targeting **Text4Shell-like vulnerabilities**.

### **Patch Management**

* Automate **dependency updates** using **AWS Systems Manager**.

### **IAM Hardening**

* **Quarterly audits** of IAM roles using **AWS IAM Access Analyzer**.
* Apply **permission boundaries** to **Lambda execution roles**.

### **Data Protection**

* Enable **S3 bucket encryption, versioning, and MFA delete**.