# **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:** ai-excelMacro-stage
* **AWS Account:** 951171340333
* **IAM Role:** LambdaExRole

### **Sensitive Resources**

* **Ignatite-license** (PII/Email data)
* **terraform-fuse-dts.us-east-Lappfire.app** (Infrastructure state)

## **1. Issue Description**

### **Overview**

* The serverless function **ai-excelMacro-stage** was **publicly exposed** via two 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 LambdaExRole**
  + Access **sensitive PII/Email data**

### **Affected Resources**

#### **Exposed Endpoints**

* https://apiai-stage.dts-bobswift.appfire.app:443/api/1.0/excel
* https://km6xcsk6k.execute-api.us-east-1.amazonaws.com:443/prod/1.0/excel

#### **Vulnerable Library**

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

#### **AWS Resources at Risk**

* **Ignatite-license** – [Link to S3 Bucket]
* **terraform-fuse-dts.us-east-Lappfire.app** – [Link to Terraform State]

### **Impact**

* **Data Breach:** Unauthorized access to **PII/Email data** in Ignatite-license.
* **Infrastructure Risk:** Manipulation of **Terraform state files** in terraform-fuse-dts.us-east-Lappfire.app.
* **Regulatory Penalties:** Potential **fines under 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 **IAM authorization** for API Gateway.
* Restricted access to **internal VPC** or **specific IP ranges**.

**Validation:**

* **Penetration testing** confirmed endpoints are no longer publicly exploitable.
* **AWS CloudTrail logs** reviewed for unauthorized access attempts.

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* **Outdated Apache Commons Text library** (v1.8).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

**Validation:**

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

### **Issue 3: Overprivileged LambdaExRole**

**Root Cause:**

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

**Fixes Implemented:**

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

**Validation:**

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

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

### **Authentication Enforcement**

* Use **AWS Cognito** or **API Keys** for API Gateway authentication.

### **Patch Management**

* Automate **dependency updates** with **AWS Lambda Layers**.

### **IAM Hardening**

* Implement **permission boundaries** for Lambda execution roles.
* Perform **quarterly audits** using **AWS IAM Access Analyzer**.

### **Data Protection**

* Enable **S3 bucket encryption** and **versioning** for critical resources.