# **Issue Document**

## **Title: Exposed Serverless Function with Critical Vulnerability (CVE-2022-42889) and Overprivileged Role**

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

## **Affected Systems/Components**

* **Serverless Function:** xl-excell Macro-stage
* **AWS Subscription:** 951171948383
* **IAM Role:** LambdaExitable

## **1. Issue Description**

### **Overview**

* The xl-excell Macro-stage serverless function was exposed via two **public endpoints** and vulnerable to **CVE-2022-42889 (Text4Shell)** due to an outdated **cernons~text library (v1.8)**.
* Attackers could exploit this to execute **arbitrary code**, escalate privileges via the overprivileged **LambdaExitable role**, and access **sensitive data** in Ignatie-itemset and terraform-fuse-dts.us-east-1.appfire.app.

### **Affected Resources**

* **Serverless Function:** xl-excell Macro-stage – [Link to AWS Lambda Console]
* **Exposed Endpoints:**
  + hxops://apis/~stage1\_lets-bedswift1\_lappfire1\_japp=443/api/v1\_10/excel
  + hxops://vmboxstack1\_jeexecute-app1\_us-east-v1\_janazanawel\_joom=443/prod/v1\_10/excel
* **AWS Resources at Risk:**
  + **Ignatie-itemset** (contains PII/email data) – [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 Ignatie-itemset.
* **Privilege Escalation:** Attacker could use **LambdaExitable role** to perform **lateral movement** in AWS subscription 951171948383.

## **2. Issue Resolution**

### **Issue 1: Initial Access via Exposed Endpoints**

**Root Cause:**

* **Public exposure** of serverless function endpoints.

**Fixes Implemented:**

* **Removed public access** to endpoints; restricted to **VPC/internal networks**.
* Enabled **AWS API Gateway authentication** (e.g., **IAM roles, API keys**).

**Validation:**

* Verified endpoints are no longer publicly accessible via **nmap scans**.
* Tested **access controls** with unauthorized requests.

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

**Root Cause:**

* **Outdated** cernons~text library (**v1.8**).

**Fixes Implemented:**

* Upgraded **library** to patched version (**>=1.10.0**).
* Scanned dependencies for **similar vulnerabilities**.

**Validation:**

* Confirmed **library version** via **AWS Lambda environment check**.
* Ran **exploit simulation tools** (e.g., **Metasploit**) to verify mitigation.

### **Issue 3: Overprivileged LambdaExitable Role**

**Root Cause:**

* **Excessive permissions** granted to LambdaExitable role.

**Fixes Implemented:**

* Revised **IAM policies** to enforce **least privilege** (e.g., **removed s3:Get\*** from non-essential buckets).
* Added **conditional access** for terraform-fuse-dts resources.

**Validation:**

* **AWS IAM Access Analyzer report** showing reduced permissions.
* **Simulated attacker workflows** blocked post-remediation.

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

### **Secure Serverless Configurations**

* **Enforce private endpoints** for Lambda functions unless public access is explicitly required.
* Use **AWS WAF** to block **malicious payloads** targeting **Text4Shell-like vulnerabilities**.

### **Patch Management**

* Automate **dependency scans** using tools like **AWS Inspector** or **Snyk**.

### **IAM Hardening**

* **Quarterly IAM role audits** using **AWS Access Analyzer**.
* Implement **permission boundaries** for Lambda execution roles.

## **4. Attachments/References**

* **CVE-2022-42889 Advisory** – [NVD Link]
* **Lambda Function Configuration** – [Link to AWS Console]
* **IAM Role Policies** – [Link to IAM Dashboard]
* **Document Version:** 1.0
* **Last Updated:** [Insert Date]