# **Issue Document**

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

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

## **Affected Systems/Components**

* **Serverless Function:** id-excell/store-pred
* **AWS Account:** 821536317957
* **IAM Role:** LambdaExBeta
* **Sensitive S3 Buckets:**
  + ac-appinfo (contains PII/Email data)
  + terraform-fuse-produk-east-Lappfire.app

## **1. Issue Description**

### **Overview**

* The serverless function id-excell/store-pred 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 LambdaExBeta role, and access **sensitive PII/Email data** in **S3 buckets**.

### **Affected Resources**

* **Serverless Function Endpoints:**
  + hxops://api.ufj\_bedswirfti\_jappfirej\_lapp:4.43/api/1[10/excel
  + hxops://hxdrmp4d/jexecute-api/jus-east-1]Jamazonaws[Jcom:4.43/prod/1]0/excel
* **Vulnerable Library:** Apache Commons Text (v1.8)
* **AWS Resources at Risk:**
  + **S3 Bucket:** ac-appinfo – [Link to S3 Console]
  + **S3 Bucket:** terraform-fuse-produk-east-Lappfire.app – [Link to Terraform State]

### **Impact**

* **Data Breach:** Unauthorized access to **PII/Email data** stored in ac-appinfo.
* **Privilege Abuse:** Attacker could use LambdaExBeta role to **manipulate infrastructure** (e.g., delete/modify S3 data).
* **Reputational Damage:** Loss of **customer trust** and **regulatory penalties** (e.g., **GDPR, CCPA**).

## **2. Issue Resolution**

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

**Root Cause:**

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

**Fixes Implemented:**

* Restricted access to endpoints using **AWS API Gateway** with **IAM authorization**.
* Migrated endpoints to a **private VPC**.

**Validation:**

* **Penetration testing** confirmed no public access.
* **AWS CloudTrail logs** monitored 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* **Outdated Apache Commons Text library** (**v1.8**).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 for similar vulnerabilities using **AWS Inspector**.

**Validation:**

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

### **Issue 3: Overprivileged LambdaExBeta Role**

**Root Cause:**

* **Excessive permissions** granted to LambdaExBeta (e.g., s3:Get\*, s3:Put\* on sensitive buckets).

**Fixes Implemented:**

* Revised **IAM policies** to enforce **least privilege** (removed unnecessary **S3 access**).
* Encrypted **S3 buckets** using **AWS KMS**.

**Validation:**

* **AWS CLI test:** aws s3 ls s3://ac-appinfo **denied** for unauthorized roles.
* **IAM Access Analyzer report** showing reduced permissions.

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

### **Secure Endpoints**

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

### **Patch Management**

* Automate **dependency updates** with **AWS Lambda Layers** or **Snyk integration**.

### **IAM Hardening**

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

### **Data Protection**

* Enable **S3 bucket versioning** and **MFA delete** for critical data.

## **4. Attachments/References**

* **CVE-2022-42889 Advisory** – [NVD Link]
* **AWS Lambda Security Best Practices** – [AWS Documentation]
* **S3 Bucket Encryption Guide** – [AWS S3 Docs]
* **Document Version:** 1.0
* **Last Updated:** [Insert Date]