# **Issue Document**

## **Title: Publicly Exposed VM with CVE-2023-0286 and Unrestricted Access to Sensitive S3 Data**

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

## **Affected Systems/Components**

* **VM:** JIRA-TESTENV\_LATEST\_SnapBytes
* **Service Account:** SSM-EC2
* **S3 Buckets at Risk:**
  + sam-tts-recalculation-state-payload-us-east-2.zip-app-csv-upload-file-ee-west-1
  + [Other buckets with financial/PII data]

## **1. Issue Description**

### **Overview**

* The VM **JIRA-TESTENV\_LATEST\_SnapBytes** was publicly exposed via **HTTP/HTTPS endpoints** and vulnerable to **CVE-2023-0286** (**Cryptography library v3.4.8**).
* The **SSM-EC2** service account had **unrestricted access** to sensitive **S3 buckets** containing **financial data (credit cards)** and **PII (names, emails, phone numbers)**.

### **Affected Resources**

* **VM Endpoints:**
  + https://44.217.995.202:443
  + http://44.217.995.202:80
* **Cryptography Library:** Version **3.4.8** (vulnerable to **CVE-2023-0286**)
* **Sensitive S3 Buckets:**
  + sam-tts-recalculation-state-payload-us-east-2.zip-app-csv-upload-file-ee-west-1 – [Link to S3 Console]
  + [Other bucket links]

### **Impact**

* **Data Breach:** Exposure of **financial data (credit cards)** and **PII** stored in S3 buckets.
* **Reputational Damage:** Loss of **customer trust** due to compromised sensitive information.
* **Regulatory Fines:** Potential penalties under **GDPR, CCPA, or PCI-DSS**.

## **2. Issue Resolution**

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

**Root Cause:**

* Publicly accessible **HTTP/HTTPS endpoints** without network restrictions.

**Fixes Implemented:**

* Restricted VM access to **internal IP ranges** using **AWS Security Groups**.
* Disabled **unnecessary public endpoints**.

**Validation:**

* nmap scans confirmed **endpoints are no longer publicly accessible**.
* **AWS CloudTrail logs** reviewed for unauthorized access attempts.

### **Issue 2: CVE-2023-0286 (Cryptography Library Vulnerability)**

**Root Cause:**

* Outdated library (**v3.4.8**) vulnerable to **code execution/information disclosure**.

**Fixes Implemented:**

* Upgraded **Cryptography library** to v**39.0.1** (patched version).

**Validation:**

* **Vulnerability scan (e.g., Nessus)** confirmed **no CVE-2023-0286 exposure**.
* **Penetration testing** verified **RCE mitigation**.

### **Issue 3: Unrestricted S3 Access via SSM-EC2 Account**

**Root Cause:**

* Overprivileged **SSM-EC2 service account** with access to **sensitive S3 buckets**.

**Fixes Implemented:**

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

**Validation:**

* **AWS CLI test:** aws s3 ls s3://sam-tts... **denied** for unauthorized roles.
* **AWS IAM Access Analyzer report** showed **reduced permissions**.

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

### **Data Encryption:**

* Enable **default encryption** for all S3 buckets using **AWS KMS**.

### **Network Hardening:**

* Use **AWS PrivateLink** for **internal service communication**.

### **IAM Policies:**

* **Quarterly audits** of service account permissions using **AWS IAM Access Analyzer**.

### **Patch Management:**

* Automate **library updates** with **AWS Systems Manager Patch Manager**.

## **4. Attachments/References**

* **CVE-2023-0286 Advisory** – [NVD Link]
* **AWS S3 Encryption Guide** – [AWS Documentation]
* **VM Configuration Backup** – [Link to Snapshot]
* **Document Version:** 1.0
* **Last Updated:** [Insert Date]