# **Issue Document**

## **Title: Publicly Exposed VM with CVE-2023-0286 and Cleartext AWS Keys Leading to PII Exposure**

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

## **Affected Systems/Components**

* **VM:** DIRA-TESTENV\_LATEST\_Snapbytes
* **Service Account:** blzsys-automations.appfire().json

### **Sensitive Data Resources:**

* appfire-email-drive-backup
* sf-dee-actracts
* sf-salesforce-extracts

## **1. Issue Description**

### **Overview**

* The VM DIRA-TESTENV\_LATEST\_Snapbytes was publicly exposed via **HTTP/HTTPS endpoints** and vulnerable to **CVE-2023-0286** in the cryptography library (**v3.4.8**).
* Attackers could **execute code**, steal **unencrypted AWS keys**, and access **sensitive data** using the overprivileged blzsys-automations.appfire().json service account.

### **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**)

#### **Exposed AWS Keys:**

* AKUANCE6BNFYNAOFISSE
* AKUAYZHYUQSHJQSX30W

#### **Sensitive Data Stores:**

* appfire-email-drive-backup (**emails, PII**) – [Link to S3 Bucket]
* sf-dee-actracts (**financial data**) – [Link to Salesforce]
* sf-salesforce-extracts (**sales records**) – [Link to Data Warehouse]

### **Impact**

* **Data Breach:** Exposure of **PII** (names, emails, phone numbers) and **financial data**.
* **Regulatory Risks:** Violations of **GDPR, CCPA, or PCI-DSS** due to leaked sensitive information.
* **Operational Disruption:** Potential **manipulation or deletion** of critical business data.

## **2. Issue Resolution**

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

**Root Cause:**

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

**Fixes Implemented:**

* Restricted access using **AWS Security Groups** (allowlisted internal IPs only).
* Disabled unnecessary ports (**80/443**).

**Validation:**

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

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

**Root Cause:**

* Outdated cryptography library (**v3.4.8**) allowing **code execution**.

**Fixes Implemented:**

* Upgraded **cryptography library** to **v39.0.1** (**patched version**).

**Validation:**

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

### **Issue 3: Cleartext AWS Keys and Overprivileged Service Account**

**Root Cause:**

* **Unencrypted AWS keys** stored on the VM.
* **Service account granted excessive permissions**.

**Fixes Implemented:**

* **Revoked compromised keys:**
  + AKUANCE6BNFYNAOFISSE
  + AKUAYZHYUQSHJQSX30W
* Enforced **least privilege** for blzsys-automations.appfire().json (**removed s3:Get\*, sf:Admin access**).
* Migrated **secrets** to **AWS Secrets Manager** with encryption.

**Validation:**

* **AWS CLI test:** aws sts get-caller-identity failed with revoked keys.
* **IAM Access Analyzer report** confirmed reduced permissions.

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

### **Secrets Management**

* Automate **AWS key rotation** using **AWS IAM Credential Rotation**.
* Encrypt all **secrets at rest** using **AWS KMS**.

### **Network Hardening**

* Deploy **AWS WAF** to block **exploit attempts** on public endpoints.

### **IAM Policies**

* Implement **permission boundaries** for **service accounts**.
* Conduct **quarterly audits** using **AWS IAM Access Analyzer**.

### **Data Protection**

* Enable **S3 bucket encryption** and **access logging** for appfire-email-drive-backup and related resources.

## **4. Attachments/References**

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