# **Issue Document**

## **Title: Publicly Exposed VM with Cryptography Vulnerability and Cleartext AWS Keys Granting Admin Privileges**

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

## **Affected Systems/Components**

* **VM:** JIRA-TESTENV\_LATEST\_Snapbytes
* **AWS Account:** bitsys-automationspappfire[.]com
* **Service Account:** bitsys-automationspappfire[.]com (admin privileges)

### **Exposed Endpoints**

* https://44.217.195.202:443
* http://44.217.195.202:80

## **1. Issue Description**

### **Overview**

A publicly exposed VM (JIRA-TESTENV\_LATEST\_Snapbytes) was found to have:

* **CVE-2023-0286** in the **cryptography library (v5.4.8)**, allowing **remote code execution (RCE)**.
* **Unencrypted AWS access keys** with **admin privileges**, enabling **privilege escalation** and **lateral movement** in AWS.

### **Affected Resources**

* **VM Dashboard:** [Link to VM Management Console]
* **AWS Access Keys Exposed:**
  + AKIAMCE6BNFYNAOFISSE
  + AKIAWANTBP2XPYYAY35N
  + AKIAYZFFVUGSHOOSXJON
* **AWS Resources at Risk:**
  + **Admin privileges** for bitsys-automationspappfire[.]com
  + **Sensitive data/workflows** in the associated AWS environment

### **Impact**

* **Data Breach:** Unauthorized access to AWS resources and **PII**.
* **Privilege Escalation:** Attacker could perform **admin-level operations** (e.g., **delete resources, create new users**).
* **Workflow Disruption:** Critical workflows could be **halted or manipulated**.

## **2. Issue Resolution**

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

**Root Cause:**

* Publicly accessible **HTTP/HTTPS endpoints** with **no network restrictions**.

**Fixes Implemented:**

* Blocked **public access** via **AWS Security Groups** or **firewall rules**.
* Migrated endpoints to a **private subnet/VPC**.

**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* Outdated **cryptography library (v5.4.8)**.

**Fixes Implemented:**

* Upgraded **library** to **v39.0.1** (patched version).
* Rebuilt **VM dependencies** to eliminate legacy components.

**Validation:**

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

### **Issue 3: Cleartext AWS Keys and Excessive Privileges**

**Root Cause:**

* **Unencrypted AWS keys** stored on the VM; **service account** granted **admin rights**.

**Fixes Implemented:**

* **Revoked compromised keys:**
  + AKIAMCE6BNFYNAOFISSE
  + AKIAWANTBP2XPYYAY35N
  + AKIAYZFFVUGSHOOSXJON
* **Enforced least privilege** for bitsys-automationspappfire[.]com (removed **admin access**).
* **Encrypted secrets** using **AWS Secrets Manager**.

**Validation:**

* **AWS IAM Access Analyzer report** showing reduced permissions.

**Verified keys are invalid via AWS CLI:** bash  
CopyEdit  
aws sts get-caller-identity --access-key-id <KEY\_ID>

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

### **Secrets Management**

* Use **AWS Secrets Manager** or **HashiCorp Vault** for credential storage.
* Automate **key rotation** every **90 days**.

### **Network Hardening**

* Enforce **VPC peering** for internal services; **disable public IPs by default**.

### **Least Privilege Enforcement**

* Apply **AWS Service Control Policies (SCPs)** to restrict **admin privileges**.

### **Patch Management**

* Automate **library updates** using tools like **AWS Systems Manager Patch Manager**.

## **4. Attachments/References**

* **CVE-2023-0286 Advisory:** [NVD Link]
* **AWS IAM Best Practices:** [AWS Documentation]
* **VM Configuration Backup:** [Link to Snapshot]
* **Document Version:** 1.0
* **Last Updated:** [Insert Date]