# **Issue Document**

## **Title: Publicly Exposed VM with High Privileges and Initial Access Vulnerabilities**

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

## **Affected Systems/Components**

* **VM:** chief-service.asp@fn.com
* **Subscription:** AppPro ITOps
* **Service Account:** ec2-default-rele

## **1. Issue Description**

### **Overview**

* A publicly exposed VM (chief-service.asp@fn.com) was found to have a high-severity vulnerability (**CVE-2023-0206**) in its cryptography library (**v3.4.6**).
* This vulnerability enables potential **remote code execution (RCE)**.
* The VM’s service account (ec2-default-rele) had **excessive permissions**, increasing the risk of **privilege escalation** and **lateral movement**.

### **Affected Resources**

* **VM:** chief-service.asp@fn.com – [Link to VM Dashboard]
* **Service Account:** ec2-default-rele – [Link to IAM Console]
* **Subscription:** AppPro ITOps – [Link to Subscription Overview]
* **Exposed Endpoints:**
  + https://24.241.37:340:3118 (restricted post-fix)

## **2. Issue Resolution**

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

**Root Cause:**

* Publicly accessible endpoints with **no IP restrictions**.

**Fixes Implemented:**

* Updated **Network Security Groups (NSGs)** to **restrict access** to internal IP ranges.
* Removed **public exposure** of endpoints.

**Validation:**

* **Penetration testing** confirmed restricted access.
* **Network traffic logs** reviewed for unauthorized attempts.

**Prevention:**

* Quarterly **firewall/NSG rule audits**.

### **Issue 2: CVE-2023-0206 Vulnerability in Cryptography Library**

**Root Cause:**

* Outdated cryptography library (**v3.4.6**).

**Fixes Implemented:**

* Upgraded **library** to secure version **39.0.1**.

**Validation:**

* **Vulnerability scan** confirmed patch compliance.
* **Functional testing** verified no breaking changes.

**Prevention:**

* Enforced **automated patch management**.

### **Issue 3: Overprivileged Service Account (ec2-default-rele)**

**Root Cause:**

* Excessive permissions (e.g., **AMS accession access**) violating **least privilege**.

**Fixes Implemented:**

* Revoked **unnecessary permissions**.
* Applied **least-privilege policies**.

**Validation:**

* **Permission audit** confirmed reduced access levels.
* **Simulated attack tests** blocked privilege escalation.

**Prevention:**

* Automated **permission audits** for service accounts.

## **3. Attachments/References**

* **CVE-2023-0206 Advisory** – [NVD Link]
* **VM Configuration Dashboard** – [Link to VM Management Portal]
* **Service Account Permissions Report** – [Link to IAM Audit]
* **Document Version:** 2.1
* **Last Updated:** [Insert Date]