# **Issue Document**

## **Title: Publicly Exposed Docker Daemon with Critical Vulnerabilities and Cleartext AWS Keys Leading to Privilege Escalation**

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

## **Affected Systems/Components**

* **VM:** Docker Daemon (http://54.76.59:145:9999)
* **AWS Account:** qoBlabs-de
* **Service Account:** DC\_Perf\_teats
* **Exposed AWS Key:** AKIAU7R0H65QDTSH4K7RB

## **1. Issue Description**

### **Overview**

* The **Docker Daemon** on the VM was publicly exposed and vulnerable to:  
  + **CVE-2023-0286** (cryptography library).
  + **CVE-2023-27043** (python3-libs).
* Attackers could exploit these vulnerabilities to:  
  + Execute **arbitrary code**.
  + Steal **unencrypted AWS keys**.
  + Use the **overprivileged service account** (DC\_Perf\_teats) to disrupt AWS resources.

### **Affected Resources**

* **Exposed Endpoint:** http://54.76.59:145:9999 (**Docker Daemon**)
* **Vulnerable Libraries:**
  + **cryptography library** (**CVE-2023-0286**)
  + **python3-libs** (**CVE-2023-27043**)
* **AWS Key at Risk:** AKIAU7R0H65QDTSH4K7RB (linked to DC\_Perf\_teats)
* **AWS Actions Possible:**
  + **Delete** DB instances.
  + **Modify** network ACLs.
  + **Alter** DNS records.

### **Impact**

* **Operational Disruption:** Critical resources (e.g., databases, DNS) could be deleted or modified.
* **Security Breach:** Unauthorized network changes enabling lateral movement.
* **Reputational Damage:** Loss of customer trust and regulatory scrutiny.

## **2. Issue Resolution**

### **Issue 1: Public Exposure of Docker Daemon**

**Root Cause:**

* Docker Daemon was **exposed to the public internet** without authentication.

**Fixes Implemented:**

* **Restricted** Docker Daemon access to internal IP ranges.
* **Enabled** TLS authentication for the Docker API.

**Validation:**

* nmap scans confirmed **port 9999** is no longer publicly accessible.
* Reviewed **Docker logs** for unauthorized access attempts.

### **Issue 2: CVE-2023-0286 and CVE-2023-27043 Exploitation**

**Root Cause:**

* **Outdated libraries** vulnerable to **RCE**.

**Fixes Implemented:**

* **Updated** cryptography library to a patched version (≥ **39.0.2**).
* **Upgraded** python3-libs to resolve **CVE-2023-27043**.

**Validation:**

* **Vulnerability scans** (e.g., **Tenable**) confirmed no CVE exposure.
* **Exploit simulations** (e.g., **Metasploit**) blocked post-patch.

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

**Root Cause:**

* **Unencrypted AWS keys** stored on the VM.
* **Service account (DC\_Perf\_teats)** granted excessive permissions.

**Fixes Implemented:**

* **Revoked compromised key:** AKIAU7R0H65QDTSH4K7RB.
* **Enforced least privilege** for DC\_Perf\_teats (e.g., revoked rds:DeleteDBInstance, route53:ChangeResourceRecordSets).
* **Migrated secrets** to **AWS Secrets Manager** with encryption.

**Validation:**

* **AWS CLI test:** aws iam list-access-keys confirmed key revocation.
* **IAM policy audit** using **AWS Access Analyzer**.

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

### **Secrets Management**

* **Automate AWS key rotation** using **AWS IAM Credential Rotation**.
* **Scan code/configurations** for hardcoded secrets using tools like **GitGuardian**.

### **Network Hardening**

* Use **AWS Security Hub** to monitor public exposure of services.
* Deploy **AWS GuardDuty** for anomaly detection.

### **Patch Management**

* **Automate OS/library updates** using **AWS Systems Manager**.

### **IAM Policies**

* Apply **AWS Service Control Policies (SCPs)** to restrict high-risk actions (e.g., rds:Delete\*).