مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Docker Desktop

Tracking #:432317640

Date:27-08-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a a critical security vulnerability in Docker Desktop for Windows and macOS that could allow an attacker to escape container isolation and gain unauthorized access to the host system.

TECHNICAL DETAILS:

Vulnerability Details:

- CVE-2025-9074
- CVSS v3.1 Score: 9.3 (Critical)
- A critical vulnerability exists in Docker Desktop for Windows and macOS allows attackers to compromise the host system by running a malicious container, even when Enhanced Container Isolation (ECI) is enabled. The issue is caused by a Server-Side Request Forgery (SSRF) flaw in the Docker Engine API.
- The vulnerability stems from improper access control on the Docker Engine API, which is exposed at 192.168.65[.]7:2375 without authentication. This flaw allows any container to communicate with the Docker Engine API and create new containers without requiring the Docker socket to be mounted.
- A malicious container could exploit this flaw to:
  - Launch new containers bound to sensitive host directories.
  - Access and modify files on the host system.
  - Escalate privileges to administrator on Windows by overwriting system DLLs.
  - On macOS, bypass some restrictions and backdoor Docker configuration files.
- **Proof-of-concept (PoC)**: Available

Impact

- **Windows:** Complete host compromise. An attacker can mount C:\ as administrator, read sensitive files, and overwrite system DLLs to escalate privileges.
- **macOS:** Limited impact compared to Windows, but attackers can modify Docker configuration and control Docker containers without user approval.

Affected Versions

- Docker Desktop for Windows (prior to 4.44.3)
- Docker Desktop for macOS (prior to 4.44.3)

Fixed Versions

- Docker Desktop version 4.44.3 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Docker.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2025-9074