مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

High-Severity Path Traversal Vulnerability in Docker Compose

Tracking #:432317874

Date:29-10-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity path traversal vulnerability in Docker Compose, impacting a wide range of environments including Docker Desktop, standalone Compose binaries, CI/CD systems, and cloud development environments.

TECHNICAL DETAILS:

A high-severity path traversal vulnerability, tracked as CVE-2025-62725 (CVSS v4 Score: 8.9), has been disclosed in the Docker Compose project. The flaw affects multiple environments including Docker Desktop, standalone Compose binaries, CI/CD pipelines, and cloud-based development environments. Successful exploitation allows attackers to overwrite arbitrary files on the host system without needing to build or run containers.

Vulnerability Details

- **CVE-2025-62725**
- CVSS v4 Score: 8.9 High
- The issue arises from Docker Compose trusting path information embedded in remote OCI (Open Container Initiative) compose artifacts. When Compose processes layers containing annotations such as com.docker.compose.extends or com.docker.compose.envfile, it joins attacker-supplied values with the local cache directory. This behavior enables attackers to craft malicious relative paths that traverse outside the cache directory and overwrite files on the host system.
- Attackers can exploit this vulnerability even through read-only commands like docker compose config or docker compose ps, which are commonly used for configuration validation or lint checking in CI pipelines. This makes the exposure significant since automation systems and developers processing untrusted OCI Compose files are particularly at risk.

Affected Versions

- < v2.40.2

Fixed Versions

- v2.40.2 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-2025-62725