EnCyb

Severity: High

Advisory Type: Security

Docker Compose Flaw: CVE-2025-62725

ADVISORY REPORT

TLP: AMBER

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

EXECUTIVE SUMMARY

A high-severity vulnerability in Docker Compose allows attackers to exploit path traversal through malicious OCI artifacts, enabling arbitrary file overwrites on the host system during routine operations.

- CVE-2025-62725
- CVSS Score: 8.9
- Affected Sector: General
- Affected Product: Docker Compose
- Severity: High
- Published Date: October 29, 2025

TECHNICAL DETAILS

The vulnerability, CVE-2025-62725, is a Path Traversal flaw in Docker Compose related to its handling of OCI artifacts.

- **Vulnerability Type:** Path Traversal, this occurs when software improperly validates file paths, allowing attackers to manipulate directory references and access or overwrite files outside the intended directory scope.
- **Root Cause:** Improper path validation in the OCI artifact handling logic, where attacker-controlled annotations (e.g., com.docker.compose.file, com.docker.compose.envfile) are concatenated with the local cache path without normalization or boundary checks.
- **Prerequisite for Exploitation:** The victim must process or reference a malicious remote OCI Compose artifact or YAML file (for example, by running commands like docker compose config or docker compose ps) that includes tampered path annotations.
- **Malicious annotation example:** The traversal sequences allow the final resolved path to escape the cache directory and target arbitrary host locations (e.g., /tmp/pwnd). "com.docker.compose.file": "../../../../../../../tmp/pwnd"

IMPACT

- Overwrite arbitrary host files (configs, scripts, system files).
- Steal or inject credentials and keys (e.g., ~/.ssh/authorized_keys).
- Tamper CI/CD pipelines and build artifacts.
- Gain remote code execution and persistent access.
- Break supply-chain trust in shared Compose artifacts.
- Privilege escalation leading to full system compromise if Compose runs with elevated permissions.

RECOMMENDATIONS

- Update to a secure version of Docker Compose (v2.40.2 or later) to eliminate the path traversal vulnerability.
- Only use trusted and verified OCI Compose artifacts from reputable or internal registries to prevent malicious file injection.
- Run Docker Compose with the principle of least privilege, avoiding root privileges and restricting write access to sensitive directories.
- Harden and isolate CI/CD environments that process Compose files to prevent compromise through automated workflows.
- Implement strong validation, monitoring, and file integrity checks to detect unauthorized file writes or path traversal attempts.

REFERENCES

- Docker Compose Vulnerability Allow Attacks To Overwrite Arbitrary Files
- Docker Compose Path Traversal (CVE-2025-62725) Allows Arbitrary File Overwrite via OCI Artifacts

SECURE, SCALE, SUCCEED WITH

CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com www.encyb.com