

Alert Bulletin

Bulletin N.:

Publication Date: 12/08/2026

Subject: Alert 2026-87 CopyEscape Vulnerability in Docker

Traffic Light Protocol (TLP): Amber

Affected product(s):

- moby/go-archive prior to 0.3.0.
- Docker Desktop prior to 4.86.0.
- Docker Sandboxes prior to 0.38.0 for the sbx cp host copy functionality.

Description

A security vulnerability identified as **CVE-2026-17106**, named **CopyEscape**, has been disclosed. It affects the mechanism used by Docker to copy files from a container to the host system via the docker cp command.

The vulnerability was discovered by researchers from **Imperva Red Team** and allows a container controlled by an attacker to manipulate the file copying process to cause Docker to write or overwrite files outside the directory originally selected by the user.

The flaw occurs within the TAR extraction process used by Docker. When a copy operation from a container is executed, the Docker daemon generates a TAR file based on the container's file system and sends it to the Docker CLI, which subsequently extracts it on the host system.

CopyEscape mainly combines two conditions:

- A race condition in the container's file system that allows the generation of an inconsistent TAR file.
- A flaw during extraction that allows following symbolic links to locations outside the target directory.

As a result, a malicious container can cause the Docker CLI to write files to arbitrary locations on the host system using the privileges of the user or process that executed docker cp.

Solution

Administrators are recommended to perform the following actions:

- Update **Docker Engine and Docker CLI to 29.7.2 or higher.**
- Update **Docker Desktop to 4.86.0 or higher.**

- Update **Docker Sandboxes to 0.38.0 or higher**.
- Ensure the use of moby/go-archive 0.3.0 or later when used directly by internal applications.
- Update Docker on developer workstations.
- Prioritize CI/CD runners that execute docker cp operations.
- Review automations that run Docker via sudo or as the root user.
- Apply the principle of least privilege to users running Docker CLI.
- Avoid using sudo docker cp unless strictly necessary.
- Do not copy files from untrusted or compromised containers directly to sensitive systems.

Additional information:

- [Imperva Threat Research – CopyEscape: Taking Over Docker Hosts with docker cp](#)
- [CVE Program – CVE-2026-17106](#)
- [Docker Desktop Release Notes](#)
- [Docker Engine Release Notes](#)
- [Docker Sandboxes Release Notes](#)