

# REPORT 8-6-2024\_\_10-28-29

I risultati grezzi di ogni scansione sono salvati all'interno della directory  
/home/ubuntu/Desktop/progetto/Docklz/results/8-6-2024\_\_10-28-29

## Configurazione di Docker

Analisi della configurazione di Docker presente nel sistema completata, trovi i risultati nel file  
DockerBenchmarkSecurity.txt

Sono stati rilevati 26 problemi nella configurazione di Docker.

Controllare nel file le voci con esito WARN e confrontare con il CIS Docker Benchmark v1.6.0

[Clicca qui per registrarti e scaricare il documento](#)

Ulteriori consigli e spiegazioni sono presenti al suo interno

## Analisi dell'immagine vmware/lightwave-toolchain-photon2:latest

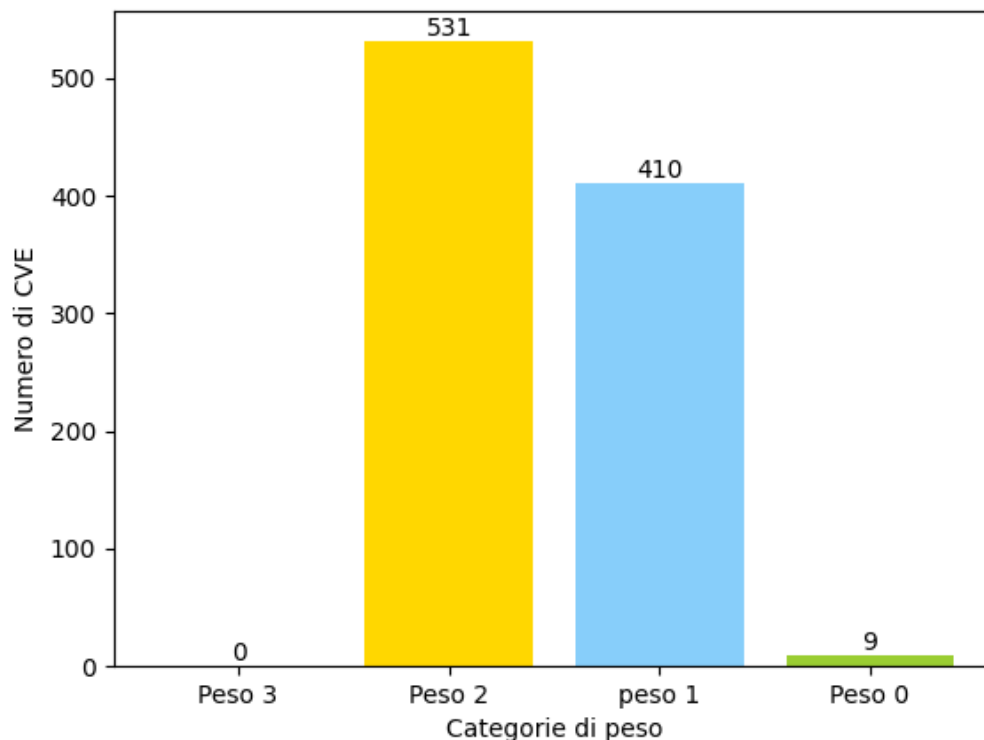
Analisi dell'immagine con Docker CLI completata, trovi i risultati nel file docker\_inspect.json.

Esso contiene varie informazioni utili per farsi un'idea iniziale dell'immagine in analisi. È importante porre l'attenzione sulle variabili d'ambiente: campo "Env", che non devono contenere alcun secret (password, key) in chiaro.

## CVE relativi all'immagine vmware/lightwave-toolchain-photon2:latest

Analisi dell'immagine con trivy completata, trovi i risultati grezzi nei file trivy\_image.txt e trivy\_image.json

Ecco un grafico che illustra i CVE analizzati, dividendoli in base al peso. Ulteriori informazioni disponibili nell'allegato  
"Allegato\_CVE.pdf"



## Analisi del codice sorgente

L'analisi del codice sorgente è stata eseguita sfruttando due tool differenti, Trivy e Semgrep.

Trovi i risultati dell'analisi con Trivy nei file trivy\_fs.txt e trivy\_fs.json

Non è stata rilevata alcuna problematica tramite questa analisi

-----

Trovi i risultati dell'analisi con Semgrep nel file semgrep\_scan.txt

Ecco le principali problematiche rilevate:

- generic secrets security detected sonarqube docs api key detected sonarqube docs api key
- javascript lang security audit path traversal path join resolve traversal path join resolve traversal