Trivy vs Snyk

Confronto tra due scanner di vulnerabilità per container

Giovanni Bellini
Matricola: 600035
ICT Risk Assessment
Corso di laurea magistrale in Informatica
Università degli Studi di Pisa

Febbraio 2024

Indice

1 Introduzione **3**
1.1 Processo di scansione 3
1.1.1 Trivy 3
1.1.2 Snyk 4

2 Confronto **6**
2.1 Scansione delle vulnerabilità 6
2.1.1 Risultati delle scansioni 7
2.1.2 Formati di output 8
2.2 Scansione di configurazioni IaC 10
2.3 Funzionalità uniche per ogni prodotto 11
2.3.1 Snyk: Monitoraggio Continuo 11
2.3.2 Trivy: scansione di immagini VM 12

Capitolo 1

Introduzione

In un'epoca in cui il software permea ogni aspetto della vita quotidiana, la sicurezza informatica è diventata una pietra angolare nello sviluppo e nel deployment delle applicazioni. La continua espansione dell'utilizzo dei container e delle microservizi ha portato alla necessità di strumenti sofisticati capaci di identificare e mitigare le vulnerabilità in modo efficace ed efficiente. Questo report si propone di esplorare e confrontare due dei più rilevanti strumenti nel panorama della sicurezza informatica: Trivy e Snyk. Entrambi gli strumenti hanno guadagnato notorietà per la loro capacità di fornire analisi dettagliate e soluzioni alle vulnerabilità di sicurezza in applicazioni e container, ma presentano approcci, caratteristiche e punti di forza distinti.

Trivy

Trivy, sviluppato da Aqua Security, è un scanner di vulnerabilità open source semplice e completo, che si distingue per la sua facilità d'uso e la capacità di integrarsi senza soluzione di continuità in vari ambienti di sviluppo e pipeline CI/CD. La sua progettazione si concentra sulla velocità e sull'efficacia della scansione di immagini di container, repository Git, filesystem e configurazioni Infrastructure as Code (IaC), rendendolo uno strumento versatile per gli sviluppatori e i team di sicurezza.

Snyk

Snyk si posiziona come una soluzione SaaS di sicurezza per lo sviluppo software che enfatizza la collaborazione tra sviluppatori e professionisti della sicurezza. Offre una vasta gamma di funzionalità che vanno oltre la semplice scansione delle vulnerabilità, inclusa la gestione delle dipendenze, la correzione automatica e l'integrazione profonda con ambienti di sviluppo, sistemi di gestione del codice sorgente e pipeline di CI/CD. Snyk mira a dotare i team di strumenti proattivi per affrontare le vulnerabilità all'interno del loro codice, delle dipendenze open source, dei container e delle configurazioni IaC.

1.1 Processo di scansione

1.1.1 Trivy

I tool effettuano il processo di scansione delle vulnerabilità in container Docker modi diversi:

Trivy utilizza il comando di scansione `trivy image` per eseguire la scansione di un'immagine Docker. Questo comando esegue automaticamente tre funzioni:

- **Download del database delle vulnerabilità**: Trivy scarica automaticamente l'ultima versione del database delle vulnerabilità dalla repository ufficiale.
- **Scansione dell'immagine**: Trivy esegue la scansione dell'immagine Docker specificata, identificando e classificando le vulnerabilità presenti nei pacchetti e nelle librerie. Nel processo di scansione, Trivy analizza i file presenti nell'immagine, identificando le versioni dei pacchetti e confrontandole con il database di vulnerabilità. Nel processo, vengono scansionate quattro categorie di problemi di sicurezza:
  - **Vulnerabilità**: problemi di sicurezza noti e documentati, che possono essere sfruttati da attaccanti per compromettere l'integrità e la disponibilità del sistema.
  - **Configurazioni errate**: errori di configurazione e di implementazione che possono esporre il sistema a rischi di sicurezza.
  - **Segreti e chiavi di accesso**: presenza di segreti e chiavi di accesso non crittografate all'interno dell'immagine, che possono essere sfruttati da attaccanti per ottenere accesso non autorizzato al sistema.
  - **Licenze:** presenza di licenze non conformi o non autorizzate all'interno dell'immagine, che possono esporre il sistema a rischi legali e di sicurezza.

  Di default, Trivy esegue la scansione di tutte e quattro le categorie, ma è possibile specificare una categoria specifica da scansionare utilizzando l'opzione `-scanners <vuln_type>`.
- **Generazione del report**: Trivy genera un report dettagliato delle vulnerabilità rilevate, classificandole in base al loro grado di gravità e fornendo informazioni dettagliate sulle azioni consigliate per mitigarle. La gravità di una vulnerabilità è assegnata tramite due fattori principali:
  - Principalmente, si fa affidamento al livello di gravità riportato dal vendor per tale vulnerabilità.
  - In caso il vendor non riporti la categoria della vulnerabilità, Trivy fa affidamento alla gravità assegnata dal database NVD.
  - In caso anche il database NVD non riporti la categoria della vulnerabilità, Trivy la riporta come di categoria UNKNOWN.

1.1.2 Snyk

Snyk opera invece secondo un processo differente, approcciando la scansione delle vulnerabilità direttamente dai momenti di stesura del codice. Esso è infatti suddiviso in quattro componenti principali:

- **Snyk Code:** componente relativo all'analisi statica. In questo passaggio, viene analizzato il codice sorgente per identificare i possibili problemi di sicurezza presenti nel codice. È possibile integrare Snyk Code con ambienti di sviluppo (es. Visual Studio Code) o sistemi di gestione del codice sorgente (es. Git), per eseguire automaticamente la scansione del codice sorgente, ad esempio all'esecuzione di un nuovo commit. Gli

eventuali problemi di sicurezza rilevati vengono notificati all'utente tramite l'interfaccia web di Snyk, con un'evidenziazione delle linee di codice interessate e delle azioni consigliate per mitigare i problemi, come riportato in figura 1.1.

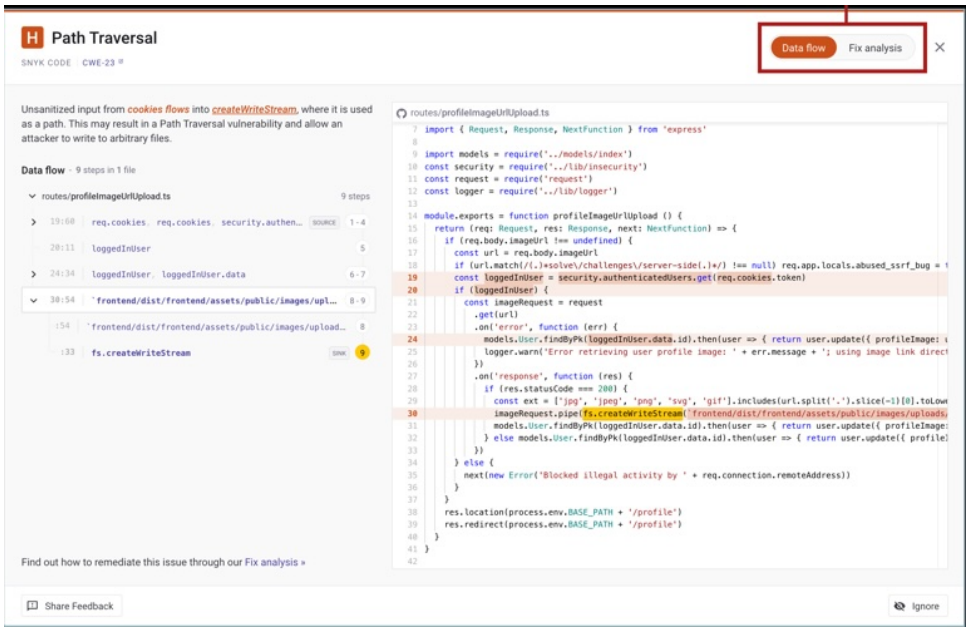

Figura 1.1: Risultato della scansione del codice sorgente con Snyk Code

- **Snyk Container:** il vero e proprio strumento per l'analisi delle vulnerabilità. Questo processo è suddiviso in tre fasi principali:
  - **Download dell'immagine**: l'immagine viene automaticamente scaricata in locale per permetterne l'analisi.
  - **Ottenimento della lista del software installato:** Snyk cerca il software installato all'interno dell'immagine. La ricerca viene effettuata in base a tre criteri:
    * Software installato tramite package manager (es. apt, yum, apk)
    * Software comunemente installato, e residente in posizioni predefinite
    * Applicazioni basate sulla presenza di un file manifest (es. package.json, requirements.txt)
  - **Invio delle vulnerabilità a Snyk:** La lista del software trovato viene inviata tramite API a Snyk, la quale confronta i dati con il suo database di vulnerabilità. Le vulnerabilità trovate vengono quindi restituite all'utente.
- **Snyk Open Source:** Snyk Open Source è uno strumento di analisi delle vulnerabilità per le dipendenze open source, che identifica e classifica le vulnerabilità presenti nelle librerie e nei pacchetti utilizzati all'interno del codice sorgente. Snyk Open Source è in grado di eseguire la scansione delle dipendenze open source, identificando le vulnerabilità e fornendo informazioni dettagliate sulle azioni consigliate per mitigarle.
- **Snyk Infrastructure as Code (IaC):** Snyk IaC è uno strumento di analisi delle vulnerabilità per le configurazioni Infrastructure as Code (IaC), che identifica e classifica le vulnerabilità presenti nei file di configurazione di Terraform, CloudFormation e altri strumenti di automazione dell'infrastruttura. Snyk IaC è in grado di eseguire la scansione delle configurazioni IaC, identificando le vulnerabilità e fornendo informazioni dettagliate sulle azioni consigliate per mitigarle.

Capitolo 2

Confronto

2.1 Scansione delle vulnerabilità

Il database di entrambi gli strumenti è un aspetto cruciale per la qualità e l'accuratezza delle analisi di vulnerabilità. Trivy e Snyk utilizzano database di vulnerabilità differenti, che influenzano la loro capacità di identificare e classificare le vulnerabilità.
In questa parte di testing, si è voluto valutare la capacità di Trivy e Snyk di identificare e classificare le vulnerabilità in base al database utilizzato. Per fare ciò, si è utilizzato un campione di immagini di container e repository Git, contenenti vulnerabilità note e ben documentate, e si è confrontato il risultato delle scansioni di Trivy e Snyk con le informazioni disponibili nei database VulnDB e Snyk. I risultati di questo test sono stati valutati in base alla precisione, alla completezza e alla tempestività delle informazioni fornite da Trivy e Snyk, e alla loro capacità di identificare e classificare le vulnerabilità in base al database utilizzato. L'aggiornamento dei database avviene per ogni tool in modo differente. Trivy, infatti, controlla la presenza di aggiornamenti del database ad ogni esecuzione, e scarica automaticamente la versione più recente. Snyk, invece, offre la possibilità di aggiornare manualmente il database, ma non è possibile controllare la presenza di aggiornamenti in modo automatico.
Le immagini Docker sottoposte a scansione sono state selezionate in base alla loro popolarità e alla loro rilevanza nel panorama delle applicazioni e dei servizi cloud. In particolare, si è scelto di testare le seguenti immagini:

- **nginx**: uno dei principali server web e reverse proxy.
- **mongo**: database NoSQL flessibile e scalabile basato su MongoDB.
- **wordpress**: piattaforma di blogging e CMS.
- **alpine**: una delle immagini di container più leggere e minimali, basata su Alpine Linux È ampiamente usata come base per altre immagini di container.
- **node**: ambiente di esecuzione per JavaScript basato su Chrome V8.

In particolare, si è voluto testare due tipi di versioni: la versione più recente, e una versione più datata. Nella tabella 2.1 sono riportati i risultati ottenuti da entrambi i tool per ciascuna immagine testata.

Immagine	Vers.	Snyk				Trivy			
		Crit.	High	Mid	Low	Crit.	High	Mid	Low
nginx	latest	1	6	3	78	2	16	34	83
	v1.23.0	10	39	73	111	16	80	139	115
mongo	latest	0	0	1	12	0	0	1	21
	v4.4.3	0	7	88	69	0	13	195	105
wordpress	latest	1	1	3	150	3	50	143	326
	v6.0.0	23	66	142	228	49	340	509	547
alpine	latest	0	0	0	0	0	0	0	0
	v3.11	1	0	0	0	1	0	0	0
node	latest	1	4	3	160	5	73	246	481
	v16.0.0	48	183	275	390	140	970	1353	1417

Tabella 2.1: Risultati delle scansioni di Snyk e Trivy per ciascuna immagine testata.

2.1.1 Risultati delle scansioni

Dai risultati ottenuti, si evincono le seguenti considerazioni:

Numero di vulnerabilità rilevate

Trivy generalmente avvisa di un numero maggiore di vulnerabilità rispetto a Snyk. Questo è particolarmente evidente per le versioni più datate delle immagini, dove Trivy rileva un numero significativamente maggiore di vulnerabilità. Da solo, il mero numero di vulnerabilità rilevate non è un indicatore della qualità o dell'accuratezza delle scansioni, per via della presenza di eventuali falsi positivi o di vulnerabilità non rilevate.

Differenza nella classificazione delle stesse vulnerabilità

Gli strumenti hanno riportato, in molti casi, una differenza nelle classificazioni delle stesse vulnerabilità. Questo è dovuto alla differenza di valutazione delle vulnerabilità da parte dei database utilizzati. In particolare, Snyk tende a classificare le vulnerabilità in modo più conservativo, assegnando un numero inferiore di vulnerabilità di livello critico e alto rispetto a Trivy. Ad esempio, per l'immagine `nginx:latest`, entrambi i tool hanno rilevato correttamente la vulnerabilità CVE-2023-6879, relativa ad un buffer overflow presente nella libreria `AOMedia`, ma mentre Trivy ha classificato la vulnerabilità come di livello critico, Snyk ha classificato la stessa come di livello basso. Questa differenza è dovuta alle sorgenti di informazioni di valutazione utilizzate dai due tool:

- Trivy utilizza la classificazione NVD, che è nota per essere meno conservativa nella classificazione delle vulnerabilità, assegnando quindi un numero maggiore di vulnerabilità di livello critico o alto.
- Snyk invece assegna la categoria in base a tre elementi di valutazione:
  - L'analisi interna condotta dal team di Snyk.
  - Una valutazione della gravità fornita dal team di sicurezza del manutentore della distribuzione Linux.
  - La gravità della vulnerabilità secondo il database NVD.

Visitando infatti il sito web `security-tracker.debian.org`, è possibile osservare che la vulnerabilità CVE-2023-6879 è stata classificata come di livello basso dal team di sicurezza di Debian, e questo ha influenzato in modo predominante la classificazione di Snyk.

Confermata di presenza di vulnerabilità ereditate

È stata inoltre confermata la presenza di vulnerabilità "ereditate" dalla Base Image: ad esempio, l'unica vulnerabilità che Snyk rileva come critica nell'ultima versione delle immagini `nginx`, `wordpress`, `node` è la stessa vulnerabilità CVE-2023-45853. Questa vulnerabilità è attualmente presente nel sistema Debian e relativa alla libreria `zlib`, ed è stata quindi ereditata dalle immagini Docker che utilizzano Debian come base image. Trivy riporta anch'esso che la vulnerabilità è critica, ma anche che ha uno stato `will_not_fix`. Ciò indica che tale vulnerabilità è conosciuta, ma al momento non ci sono piani per una correzione. Snyk non riporta invece tale informazione.

2.1.2 Formati di output

Entrambi gli strumenti offrono la possibilità di generare report in vari formati per permetterne, ad esempio, l'integrazione diretta con altri strumenti.

Trivy

Il formato di output di default di Trivy è il formato tabulare (Figura 2.1), che fornisce un report strutturato e facilmente leggibile delle vulnerabilità rilevate.

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
Flask (METADATA)	CVE-2023-30861	HIGH	fixed	2.2.2	2.3.2, 2.2.5	flask: Possible disclosure of permanent session cookie due to missing Vary: Cookie... https://avd.aquasec.com/nvd/cve-2023-30861
Jinja2 (METADATA)	CVE-2024-22195	MEDIUM		3.1.2	3.1.3	jinja2: HTML attribute injection when passing user input as keys to xmlattr... https://avd.aquasec.com/nvd/cve-2024-22195
Werkzeug (METADATA)	CVE-2023-25577	HIGH		2.2.2	2.2.3	python-werkzeug: high resource usage when parsing multipart fields... https://avd.aquasec.com/nvd/cve-2023-25577
	CVE-2023-46136	MEDIUM			3.0.1, 2.3.8	python-werkzeug: high resource consumption leading to denial of service https://avd.aquasec.com/nvd/cve-2023-46136
	CVE-2023-23934	LOW			2.2.3	python-werkzeug: cookie prefixed with = can shadow unprefixed cookie https://avd.aquasec.com/nvd/cve-2023-23934
certifi (METADATA)	CVE-2023-37920	HIGH		2022.9.24	2023.7.22	python-certifi: Removal of e-Tugra root certificate https://avd.aquasec.com/nvd/cve-2023-37920
	CVE-2022-23491	MEDIUM			2022.12.07	python-certifi: untrusted root certificates https://avd.aquasec.com/nvd/cve-2022-23491
gevent (METADATA)	CVE-2023-41419	CRITICAL		22.10.2	23.9.0	python-gevent: privilege escalation via a crafted script to the WSGIServer component

Figura 2.1: Formato di output di default di Trivy

Inoltre, Trivy permette di generare report nei seguenti formati:

- **JSON**
- **JUnit XML**: un formato di output standard per i risultati dei test.
- **Sarif**: un formato di output standard per gli strumenti di analisi statica del codice.
- **Personalizzato**: se i formati predefiniti non soddisfano le esigenze, è possibile specificare un formato di output completamente personalizzato.

Snyk

Nel formato di default, Snyk restituisce un report in formato "lista" (Figura 2.2), con l'elenco di tutte le vulnerabilità rilevate.

```
Testing nginx...

✗ Low severity vulnerability found in util-linux/libblkid1
  Description: Information Exposure
  Info: https://security.snyk.io/vuln/SNYK-DEBIAN12-UTILLINUX-2401083
  Introduced through: util-linux/libblkid1@2.38.1-5+b1, e2fsprogs@1.47.0-2, util-linux/libmount1@2.38.1-5+b1,
util-linux/mount@2.38.1-5+b1, util-linux/util-linux@2.38.1-5+b1, util-linux/libuuid1@2.38.1-5+b1, util-linux/b
sdutils@1:2.38.1-5+b1, util-linux/libsmartcols1@2.38.1-5+b1, util-linux/util-linux-extra@2.38.1-5+b1
  From: util-linux/libblkid1@2.38.1-5+b1
  From: e2fsprogs@1.47.0-2 > util-linux/libblkid1@2.38.1-5+b1
  From: util-linux/libmount1@2.38.1-5+b1 > util-linux/libblkid1@2.38.1-5+b1
  and 17 more...

✗ Low severity vulnerability found in tiff/libtiff6
  Description: Missing Release of Resource after Effective Lifetime
  Info: https://security.snyk.io/vuln/SNYK-DEBIAN12-TIFF-1560922
  Introduced through: nginx-module-image-filter@1.25.3-1~bookworm
  From: nginx-module-image-filter@1.25.3-1~bookworm > libgd2/libgd3@2.3.3-9 > tiff/libtiff6@4.5.0-6+deb12u1
```

Figura 2.2: Formato di output di default di Snyk

Inoltre, vengono mostrati anche:

- Il numero totale di vulnerabilità rilevate.
- **Consigli per la base image**: Snyk propone una base image successiva o alternativa, per notificare l'utente che aggiornando la base image alcune delle vulnerabilità rilevate siano state risolte (Figura 2.3).

```
Tested 142 dependencies for known issues, found 233 issues.

Base Image    Vulnerabilities  Severity
nginx:1.23.0  233              10 critical, 39 high, 73 medium, 111 low

Recommendations for base image upgrade:

Minor upgrades
Base Image    Vulnerabilities  Severity
nginx:1.25.3  80               1 critical, 1 high, 1 medium, 77 low

Alternative image types
Base Image                  Vulnerabilities  Severity
nginx:1.25.4-bookworm-perl  80               1 critical, 1 high, 1 medium, 77 low
nginx:stable                115              2 critical, 4 high, 4 medium, 105 low
nginx:1.24.0-perl           115              2 critical, 4 high, 4 medium, 105 low
nginx:1.25.0-bullseye-perl  144              3 critical, 13 high, 20 medium, 108 low
```

Figura 2.3: Snyk: Consigli per una base image alternativa.

Inoltre, Snyk permette di generare report nei seguenti formati:

- JSON
- SARIF

Differentemente da Trivy, Snyk non permette di generare report in formati tabellari o personalizzati.

2.2 Scansione di configurazioni IaC

Un'altra funzionalità offerta da entrambi i tool è relativa alla scansione di configurazioni IaC, al fine di rilevare problemi di sicurezza o cattive pratiche di configurazione. Per testare tale funzionalità, si è utilizzato un campione di file di configurazione di Terraform, appropriatamente configurato con una vulnerabilità di esempio nota e ben documentata. Il codice in questione è il seguente:

```
provider "aws" {
   region = "us-east-1"
 }

 resource "aws_s3_bucket" "bucket_insecure" {
   bucket = "my-insecure-bucket"
   acl    = "public-read"

   tags = {
     Name        = "Insecure Bucket"
     Environment = "Test"
   }
 }
```

La vulnerabilità in questione è rappresentata dalla configurazione errata delle politiche di accesso su un bucket S3 di AWS, il quale è stato impostato per permettere l'accesso in lettura al pubblico di tutto il bucket (public-read). Tale configurazione espone i dati contenuti nel bucket a potenziali accessi non autorizzati, rappresentando un rischio significativo per la sicurezza dei dati. Eseguendo la scansione del codice soprastante con entrambi gli strumenti, sono state rilevate le seguenti vulnerabilità:

Strumento	Critical	High	Medium	Low
Snyk	0	0	1	3
Trivy	0	7	1	2

Tra le vulnerabilità rilevate, in entrambi i casi è stata rilevata la vulnerabilità desiderata. Su Snyk, la vulnerabilità è stata classificata come l'unica di livello medio. Trivy, invece, ha classificato la vulnerabilità come di livello alto. Questa differenza è dovuta alla diversa classificazione delle vulnerabilità da parte dei database utilizzati, come già discusso in precedenza. Le altre vulnerabilità di livello alto rilevate da Trivy sono state:

- Quattro vulnerabilità molto simili tra loro, relative alla mancanza di ACLs sul bucket S3. (No public access block so not blocking public acls)
- **Bucket does not have encryption enabled:** Questa vulnerabilità è stata rilevata in quanto il bucket S3 non ha configurato correttamente la cifratura dei dati.
- **Bucket does not encrypt data with a customer managed key:** Questa vulnerabilità è stata rilevata in quanto il bucket S3 non ha una configurazione per la cifratura dei dati con una chiave gestita dal cliente.

Figura 2.4: Trivy: corretto riconoscimento della vulnerabilità public-read

Questi errori non sono stati rilevati da Snyk, che però ha rilevato due possibili vulnerabilità di livello basso non rilevate invece da Trivy:

- **S3 bucket MFA delete control disabled:** Questa vulnerabilità è stata rilevata in quanto il bucket S3 non ha configurato correttamente il controllo Multi-Factor Authentication per la cancellazione dei dati.
- **S3 server access logging is disabled:** Questa vulnerabilità è stata rilevata in quanto il bucket S3 non ha configurato correttamente il logging degli accessi al server.

2.3 Funzionalità uniche per ogni prodotto

Durante il testing, sono state rilevate inoltre le funzionalità presenti in uno dei due strumenti, ma non nell'altro. Le funzionalità sono descritte di seguito. Essendo uniche per ogni prodotto, non è stato possibile confrontarle direttamente.

2.3.1 Snyk: Monitoraggio Continuo

Snyk offre un monitoraggio continuo delle applicazioni e delle dipendenze, inviando notifiche in tempo reale in caso di nuove vulnerabilità che influenzano il codice già in uso. Questo assicura che i team possano reagire rapidamente a nuove minacce. Durante il testing, è stato possibile osservare il funzionamento di questa funzione, avendo ricevuto e-mail contenenti nuove vulnerabilità pubblicate solamente giorni prima, come riportato in figura 2.5.

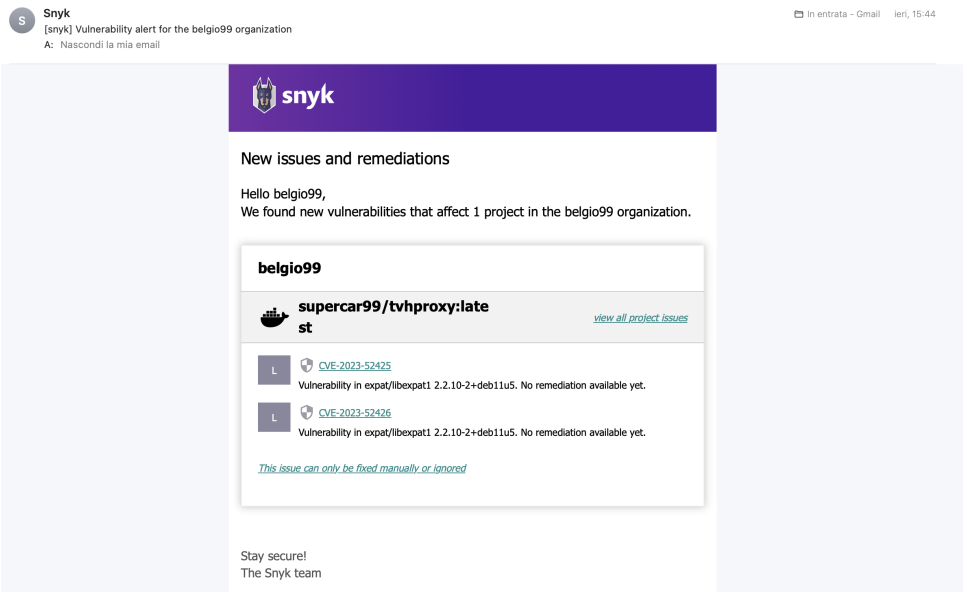

Figura 2.5: E-mail ricevuta da Snyk contenente notifica di rilevazione di nuove vulnerabilità

Dopo la ricezione della e-mail, è stata subito eseguita una scansione con Trivy, che ha confermato la presenza delle vulnerabilità segnalate da Snyk. Questo ha permesso quindi automaticamente di verificare anche la tempestività dell'aggiornamento dei database di vulnerabilità di entrambi gli strumenti.

2.3.2 Trivy: scansione di immagini VM

D'altro canto, una funzione unica di Trivy è quella di poter eseguire la scansione di immagini di macchine virtuali, oltre che di immagini di container. Tramite il comando `trivy vm`, è possibile scansionare:

- **File di macchine virtuali locali**: è supportata la scansione di file `.vmdk`
- **Cluster AWS EC2**: è supportata sia la scansione di AMI (Amazon Machine Image), sia eventuali immagini memorizzate come snapshot EBS (Elastic Block Storage)

Tale funzionalità rimane, al momento della stesura del presente report, come funzionalità sperimentale.