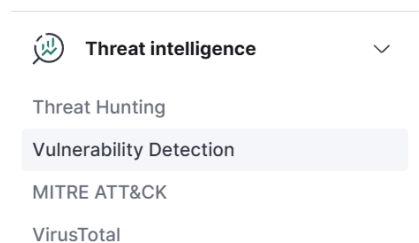


VULNERABILITY DETECTION

La funzione di **rilevamento delle vulnerabilità** in Wazuh è progettata per identificare potenziali debolezze di sicurezza negli endpoint monitorati. Utilizzando database di vulnerabilità e una scansione in tempo reale, Wazuh fornisce informazioni utili per mitigare i rischi prima che vengano sfruttati. Questa funzionalità aiuta le organizzazioni a mantenere una difesa informatica robusta, identificando software obsoleti, configurazioni errate e vulnerabilità note su diverse piattaforme.

Per attivare tale funzione configuriamo il file `ossec.conf` in modo da abilitare la vulnerability detection, fatto ciò procediamo col restart del servizio "wazuh-manager".

Ora se andiamo nella sezione "Vulnerability Detection" di Wazuh



troveremo tutte le informazioni relative alle vulnerabilità di un determinato endpoint

A screenshot of the Wazuh Vulnerability Detection dashboard. The dashboard shows a search bar with 'wazuh.cluster.name: ecommerceserver' and 'agent.id: 002'. Below the search bar, there are four large cards showing severity counts: 12 Critical, 257 High, 686 Medium, and 23 Low. Below these cards, there are four tables: 'Top 5 vulnerabilities', 'Top 5 OS', 'Top 5 agents', and 'Top 5 packages'. Each table has columns for the item name and its count.

Top 5 vulnerabilities	Count
CVE-2024-9632	5
CVE-2024-3661	4
CVE-2024-46951	4
CVE-2024-46952	4
CVE-2024-46953	4

Top 5 OS	Count
Ubuntu 22.04.5 LTS (Jammy Jellyfish)	1,558

Top 5 agents	Count
ubuntucione	1,558

Top 5 packages	Count
linux-image-6.2.0-3	656
linux-image-6.8.0-4	656
firefox	87
thunderbird	26
bluez	19

e nell'inventory possiamo vedere i dettagli di queste:

W.

Vulnerability De...

ubuntucione

a

DashboardInventoryEvents

ubuntucione (002)

Search

DQL

Refresh

wazuh.cluster.name: ecommerceserver

agent.id: 002

+ Add filter

1,558 hits

Export Formatted

44 columns hidden

Density

Sort fields

Full screen

agent.name	package.name	package.version	vulnerability.description	vulnerability.severity	vulnerability.id
ubuntucione	linux-image-6.2.0-35-gene...	6.2.0-35.35~22.04.1	In the Linux kernel, the foll...	High	CVE-2024-50262
ubuntucione	linux-image-6.2.0-35-gene...	6.2.0-35.35~22.04.1	In the Linux kernel, the foll...	Medium	CVE-2024-50258
ubuntucione	linux-image-6.2.0-35-gene...	6.2.0-35.35~22.04.1	In the Linux kernel, the foll...	High	CVE-2024-50242

Vulnerability details

t package.type	deb
t package.version	6.2.0-35.35~22.04.1
t vulnerability.category	Packages
t vulnerability.classification	CVSS
t vulnerability.description	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix out-of-bounds write in trie _get_next_key() trie_get_next_key() allocates a no de stack with size trie->max_prefixlen, while it wri tes (trie->max_prefixlen + 1) nodes to the stack w hen it has full paths from the root to leaves. For ex
vulnerability.detected_at	Nov 20, 2024 @ 22:57:39.443
t vulnerability.enumeration	CVE
t vulnerability.id	CVE-2024-50262
vulnerability.published_at	Nov 9, 2024 @ 12:15:11.000

o nel caso consultare la documentazione del NIST:

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

VULNERABILITIES

CVE-2024-38541 Detail

AWAITING ANALYSIS

This vulnerability is currently awaiting analysis.

QUICK INFO

CVE Dictionary Entry:

CVE-2024-38541