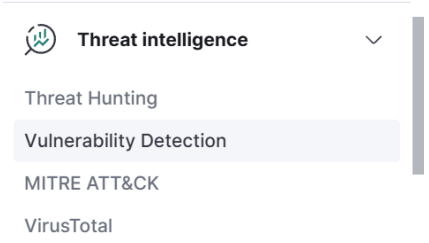
VULNERABILITY DETECTION

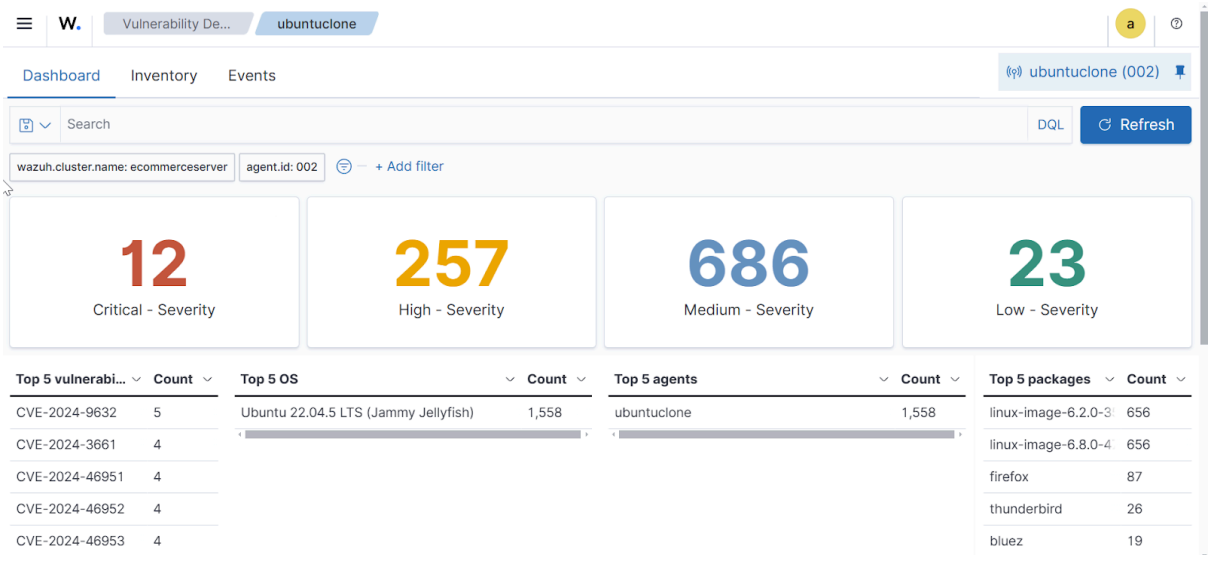
La funzione di **rilevamento delle vulnerabilità** in Wazuh è progettata per identificare potenziali debolezze di sicurezza negli endpoint monitorati. Utilizzando database di vulnerabilità e una scansione in tempo reale, Wazuh fornisce informazioni utili per mitigare i rischi prima che vengano sfruttati. 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".

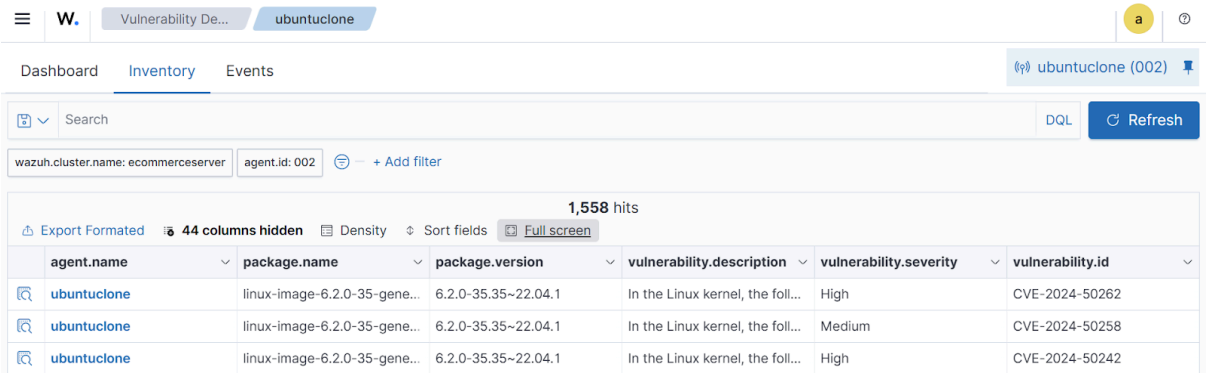
Ora se andiamo nella sezione “Vulnerability Detection” di Wazuh

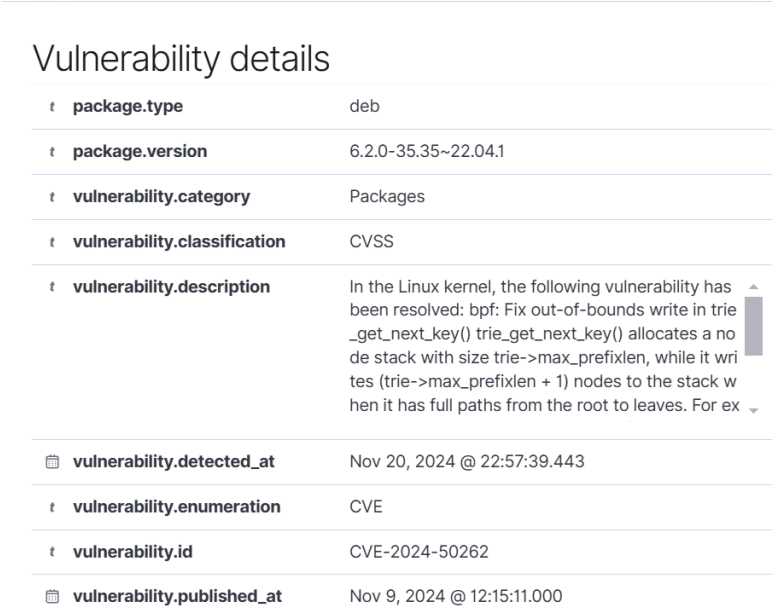


troveremo tutte le informazioni relative alle vulnerabilità di un determinato endpoint



e nell'inventory possiamo vedere i dettagli di queste:





o nel caso consultare la documentazione del NIST: