**Principali Vulnerabilità di Kubernetes e Strategie di Mitigazione**

CVE-2024-7646: Ingress-nginx Annotation Validation Bypass

- **Descrizione**: Questa vulnerabilità permette agli attaccanti di bypassare le validazioni delle annotazioni, potenzialmente esponendo il sistema a configurazioni non sicure.
- **Mitigazione**: Aggiornare all'ultima versione di ingress-nginx e applicare regole di validazione più rigide.

CVE-2024-5321: Permessi errati sui log dei container Windows

- **Descrizione**: I log dei container Windows possono avere permessi errati, permettendo l'accesso non autorizzato ai dati sensibili.
- **Mitigazione**: Configurare correttamente i permessi sui log e utilizzare strumenti di monitoraggio per rilevare accessi non autorizzati.

CVE-2024-3744: azure-file-csi-driver espone i token degli account di servizio nei log

- **Descrizione**: Questa vulnerabilità espone i token degli account di servizio nei log, permettendo potenzialmente l'accesso non autorizzato.
- **Mitigazione**: Aggiornare il driver azure-file-csi e configurare i log per escludere informazioni sensibili.

CVE-2024-3177: Bypass della policy dei segreti montabili imposta dal plugin di ammissione ServiceAccount

- **Descrizione**: Gli attaccanti possono bypassare le policy dei segreti montabili, accedendo a dati sensibili.
- **Mitigazione**: Implementare controlli di accesso più rigidi e aggiornare il plugin di ammissione ServiceAccount.

CVE-2023-5528: Sanitizzazione insufficiente degli input nel plugin di storage in-tree porta a un'escalation dei privilegi sui nodi Windows

- **Descrizione**: Input non sanitizzati correttamente possono portare a un'escalation dei privilegi sui nodi Windows.
- **Mitigazione**: Aggiornare il plugin di storage e implementare una sanitizzazione più rigorosa degli input.
    - 