Privilege escalation in Linux per un bug nel kernel

Un errore nei gruppi di controllo permette a utenti senza privilegi di uscire dai container ed eseguire comandi arbitrari nel kernel.

Due ricercatori di **Huawei**, Yiqi Sun e Kevin Wang, hanno scoperto una **vulnerabilità nella funzionalità gruppi di controllo (cgroups v1)** del kernel Linux che può permettere a un pirata di **uscire dai container, scalare i privilegi ed eseguire comandi arbitrari nella macchina host**, secondo quanto riportato da un articolo di Threatpost.

Il bug **(CVE-2022-0492) si trova nella funzionalità "cgroup_release_agent_write" del kernel**, che è in "kernel/cgroup/cgroup-v1.c". I ricercatori hanno scoperto che permette di uscire dai contenitori in ambienti **Kubernetes**, il che consente di **accedere a container di altri utenti in ambienti cloud pubblici**.

Normalmente i container offrono un buon livello di sicurezza isolando i diversi processi ma recenti incidenti hanno dimostrato che sono spesso sfruttati a causa di queste vulnerabilità.

I gruppi di controllo Linux consentono di allocare risorse del computer, come per esempio memoria e banda, tra i vari processi eseguiti sulla macchina, organizzandoli in gruppi

gerarchici. Permettono così all'utente un **controllo granulare sulla gestione e il monitoraggio delle risorse di sistema**.

Il fatto che consentano di allocare, negare, gestire e monitorare le risorse di sistema, oltre che di allocarne la priorità, rende d'altro canto questi controlli uno **strumento potente per attaccare la sicurezza**. Ci sono due tipi di architettura, **v1** e **v2**, e il bug è relativo solo al primo.

I ricercatori di Palo Alto Networks hanno pubblicato un'analisi dettagliata con patch per il problema. Il 4 febbraio, inoltre, un ricercatore ha riportato che **il bug è stato risolto**.

https://www.securityinfo.it/2022/03/09/privilege-escalation-in-linux-per-un-bug-nel-kernel/?utm_source=rss&utm_medium=rss&utm_campaign=privilege-escalation-in-linux-per-un-bug-nel-kernel