Theory: CVE-2021-25741 Symlink exchange Allow Host Filesystem Access

CVE-2021-25741 is a vulnerability that allows users to create a container with subpath volume mounts to access files & directories outside of the volume, including the host filesystem.

CVE-2021-25741 affects kubelet in these Kubernetes versions:

- v1.22.0 – v1.22.1
- v1.21.0 – v1.21.4
- v1.20.0 – v1.20.10
- <= v1.19.14

Do not print this page. This is property of the Securitydojo Powered by virtual Cybertron.

Theory

CVE-2021-25741 is a vulnerability that affects the subPath feature in Kubernetes. In Kubernetes, volumes are directories accessible to containers within a pod. The subPath volume type is used when multiple containers within a pod need to share the same volume for different purposes.

The vulnerability lies in the way subPath mounting is handled by the kubelet volume manager. When a container is launched, the kubelet mounts the required volumes and communicates the volume paths to the container. This information includes the path of the volume within the container and the path on the host system.

Using this information, the container creates the corresponding path within its filesystem and binds it to the provided host path. This binding results in the replication of the container's filesystem within the host's filesystem. Any changes made within the container's filesystem are immediately reflected in the host's filesystem.

However, in the case of subPath mounting, Kubernetes mounts the volume and performs bind mounting of the subpath. This can lead to a vulnerability where a symlink exchange occurs. Since the mount operation is controlled by the container and potentially by malicious users, this vulnerability allows for unauthorized access or manipulation of files and directories outside the intended scope.

It is important to address this vulnerability by ensuring proper security measures are in

place to prevent unauthorized symlink exchanges and limit the potential impact of malicious actions on the host system.

Reference: https://github.com/Betep0k/CVE-2021-25741/tree/main

Do not print this page. This is property of the Securitydojo Powered by Virtual Cybertron.