BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-54
Fecha de publicación: 15/10/2024
Tema: Vulnerabilidades en Imágenes de Kubernetes: CVE-2024-9486 y CVE-2024-9594
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- Versiones de Kubernetes Image Builder <= v0.1.37

Esta vulnerabilidad aplica solo si estás utilizando Kubernetes Image Builder

- CVE-2024-9486
  - Proxmox
- CVE-2024-9594
  - Nutanix, OVA, QEMU

Descripción

Las vulnerabilidades CVE-2024-9486 y CVE-2024-9594, detectadas en el proceso de creación de imágenes en Kubernetes, se deben al uso de credenciales predeterminadas que pueden exponer los sistemas a accesos no autorizados y manipulación.

La vulnerabilidad **CVE-2024-9486**, con una puntuación CVSS de 9.8, afecta las imágenes de máquinas virtuales generadas en **Proxmox**. Esta falla radica en que las credenciales predeterminadas no se deshabilitan, permitiendo que un atacante con acceso a estas pueda tomar control completo del sistema, lo que representa un riesgo crítico.

Por otro lado, la vulnerabilidad **CVE-2024-9594**, con una puntuación CVSS de 6.3, afecta las imágenes creadas con proveedores como **Nutanix, OVA, QEMU** y entornos sin procesamiento. Aunque en estos casos las credenciales predeterminadas se deshabilitan al finalizar la creación, existe una ventana de riesgo durante el proceso de construcción de la imagen.

Solución

Actualizar a la versión 0.1.38 del generador de imágenes de Kubernetes.

Información adicional:

- https://securityonline.info/cve-2024-9486-cvss-9-8-kubernetes-image-builder-flaw-exposes-vms-to-root-access/#google_vignette
- https://github.com/kubernetes/kubernetes/issues/128006
- https://github.com/kubernetes/kubernetes/issues/128007
- https://kubernetes.io/blog/

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com