Se ha revelado una vulnerabilidad crítica en Kubernetes Image Builder que, si es explotada con éxito, podría permitir obtener acceso de administrador (root) bajo ciertas condiciones.

Esta vulnerabilidad, identificada como CVE-2024-9486 (con una calificación CVSS de 9.8), ha sido corregida en la versión 0.1.38. Los encargados del proyecto agradecieron a Nicolai Rybnikar por descubrir y reportar este fallo.

> *«Se detectó un problema de seguridad en Kubernetes Image Builder, donde se habilitan credenciales predeterminadas durante el proceso de creación de imágenes»*, señaló Joel Smith de Red Hat en una alerta.
>
> *«Además, las imágenes de máquinas virtuales generadas utilizando el proveedor Proxmox no deshabilitan estas credenciales por defecto, lo que significa que los nodos que empleen estas imágenes podrían ser accesibles a través de dichas credenciales. Estas pueden ser usadas para obtener privilegios de administrador».*

Cabe señalar que los clústeres de Kubernetes solo están expuestos a este problema si sus nodos utilizan imágenes de máquinas virtuales (VM) creadas mediante el proyecto Image Builder y el proveedor Proxmox.

Como soluciones temporales, se recomienda desactivar la cuenta del constructor en las máquinas virtuales afectadas. Asimismo, se sugiere a los usuarios reconstruir las imágenes afectadas utilizando una versión corregida de Image Builder y desplegarlas nuevamente en las VM.

La solución implementada por el equipo de Kubernetes elimina las credenciales predeterminadas, reemplazándolas por una contraseña generada aleatoriamente que se utiliza durante la construcción de la imagen. Además, la cuenta del constructor se desactiva al finalizar el proceso de creación de la imagen.

La versión 0.1.38 de Kubernetes Image Builder también corrige otro problema (CVE-2024-9594, con un puntaje CVSS de 6.3) relacionado con el uso de credenciales predeterminadas cuando se crean imágenes utilizando los proveedores Nutanix, OVA, QEMU o raw.

La menor gravedad de CVE-2024-9594 se debe a que las VM que usan imágenes construidas con estos proveedores solo estarían afectadas *«si un atacante lograra acceder a la VM durante el proceso de creación de la imagen y modificara la imagen en ese momento».*

Este desarrollo coincide con la publicación de parches por parte de Microsoft para tres vulnerabilidades críticas en Dataverse, Imagine Cup y Power Platform, que podrían causar una escalada de privilegios y la exposición de información:

- CVE-2024-38139 (CVSS 8.7): Un fallo en la autenticación de Microsoft Dataverse que permite a un atacante autorizado aumentar privilegios a través de la red.
- CVE-2024-38204 (CVSS 7.5): Un problema de control de acceso en Imagine Cup que permite a un atacante autorizado obtener más privilegios por red.
- CVE-2024-38190 (CVSS 8.6): Falta de autorización en Power Platform que facilita a un atacante no autenticado visualizar información sensible a través de un ataque en red.

Esto también sigue a la divulgación de una vulnerabilidad crítica en el motor de búsqueda empresarial Apache Solr (CVE-2024-45216, puntaje CVSS: 9.8), que podría permitir la omisión de autenticación en instancias vulnerables.

> *«Un final falso en cualquier URL de la API de Solr permite que las solicitudes eviten la autenticación, manteniendo el contrato de la API con la ruta original. Este final falso parece una ruta no protegida de la API, pero se elimina internamente tras la autenticación, antes de enrutar la API»,* indicó un aviso en GitHub sobre el fallo.

El problema, que afecta a las versiones de Solr desde la 5.3.0 hasta la 8.11.4, y desde la 9.0.0 hasta la 9.7.0, ha sido solucionado en las versiones 8.11.4 y 9.7.0.