Microsoft ha alertado que el uso de plantillas preconfiguradas, como los charts de Helm incluidos de forma predeterminada, durante las implementaciones en Kubernetes, puede dar lugar a configuraciones incorrectas y a la exposición de información sensible.

> *"Estas soluciones 'listas para usar' facilitan mucho la configuración inicial, pero suelen priorizar la simplicidad por encima de la seguridad"*, explicaron Michael Katchinskiy y Yossi Weizman, del equipo de investigación de Microsoft Defender for Cloud.

Como consecuencia, muchas aplicaciones terminan siendo implementadas con configuraciones poco seguras, lo que deja expuestos datos sensibles, recursos en la nube o incluso entornos completos ante posibles atacantes.

Helm es una herramienta de gestión de paquetes para Kubernetes que permite a los desarrolladores empaquetar, configurar e implementar aplicaciones y servicios dentro de clústeres de Kubernetes. Es un proyecto respaldado por la Cloud Native Computing Foundation (CNCF).

Los paquetes de aplicaciones para Kubernetes se presentan en el formato de Helm, denominado charts, que consisten en manifiestos YAML y plantillas que describen los recursos y configuraciones necesarios para desplegar una aplicación.

Microsoft señala que muchos proyectos de código abierto incluyen manifiestos predeterminados o charts predefinidos que favorecen la facilidad de uso a costa de la seguridad. Esto suele derivar en dos problemas principales:

- Servicios expuestos al exterior sin restricciones de red adecuadas
- Falta de autenticación y autorización integradas por defecto

Por lo tanto, si las organizaciones utilizan estos recursos sin revisar cuidadosamente los manifiestos YAML y los charts de Helm, pueden acabar exponiendo sus aplicaciones a

ataques. Esto es especialmente grave cuando la aplicación desplegada tiene acceso a APIs sensibles o permite realizar acciones administrativas.

Algunos de los proyectos identificados que podrían comprometer entornos de Kubernetes incluyen:

- Apache Pinot, que expone componentes clave como `pinot-controller` y `pinot-broker` a través de servicios LoadBalancer, sin mecanismos de autenticación por defecto.
- Meshery, cuya interfaz está accesible mediante una IP externa, permitiendo que cualquier usuario cree una cuenta, acceda a la aplicación y despliegue pods, lo cual puede llevar a la ejecución de código arbitrario.
- Selenium Grid, que habilita un servicio NodePort en todos los nodos del clúster, dejando como única protección a las reglas del cortafuegos externo.

Para reducir estos riesgos, se recomienda ajustar las configuraciones siguiendo prácticas de seguridad, realizar análisis periódicos de interfaces públicas y supervisar los contenedores en ejecución para detectar actividades sospechosas o maliciosas.

> *"Muchas de las explotaciones reales contra aplicaciones en contenedores se deben a configuraciones erróneas, frecuentemente originadas por el uso de ajustes predeterminados. Confiar en configuraciones por defecto por conveniencia representa un riesgo de seguridad considerable",* concluyeron los investigadores.