Investigadores en ciberseguridad han advertido sobre imágenes maliciosas distribuidas en el repositorio oficial de Docker Hub «checkmarx/kics«.

En un aviso publicado hoy, la empresa de seguridad de la cadena de suministro de software Socket informó que actores de amenaza desconocidos lograron sobrescribir etiquetas existentes, incluidas v2.1.20 y alpine, además de introducir una nueva etiqueta v2.1.21 que no corresponde a una versión oficial. El repositorio de Docker fue archivado al momento de redactar esto.

«El análisis de la imagen comprometida indica que el binario KICS incluido fue alterado para incorporar capacidades de recopilación de datos y exfiltración que no están presentes en la versión legítima», señaló Socket.

«El malware podía generar un informe de escaneo sin censura, cifrarlo y enviarlo a un endpoint externo, creando un riesgo significativo para los equipos que utilizan KICS para analizar archivos de infraestructura como código que podrían contener credenciales u otros datos de configuración sensibles.»

Un análisis adicional del incidente reveló que herramientas relacionadas para desarrolladores de Checkmarx también podrían haber sido afectadas, como versiones recientes de la extensión de Microsoft Visual Studio Code que incluyen código malicioso para descargar y ejecutar un complemento remoto mediante el entorno Bun.

«Este comportamiento se observó en las versiones 1.17.0 y 1.19.0, fue eliminado en la 1.18.0, y dependía de una URL de GitHub codificada de forma fija para obtener y ejecutar JavaScript adicional sin confirmación del usuario ni verificación de integridad», añadió Socket.

Las organizaciones que hayan utilizado la imagen comprometida de KICS para analizar configuraciones de Terraform, CloudFormation o Kubernetes deberían considerar que cualquier secreto o credencial expuesto durante esos análisis podría haber sido comprometido.

«La evidencia sugiere que no se trata de un incidente aislado en Docker Hub, sino de una vulneración más amplia de la cadena de suministro que afecta a múltiples canales de distribución de Checkmarx», destacó la compañía.