Publicado en España el 13/03/2019

Check Point alerta sobre los peligros de la nueva vulnerabilidad en la nube en runC de Docker

Esta vulnerabilidad permite sobrescribir el host runC para poder ejecutar comandos en contenedores que ya existen o en nuevos que controlan los cibercriminales

Check Point® Software Technologies Ltd. (NASDAQ: CHKP), proveedor líder especializado en ciberseguridad a nivel mundial, alerta de una vulnerabilidad crítica en el binario runC de Linux descubierta por los investigadores Adam Iwaniuk y Borys Poplawski. Esta vulnerabilidad permite al cibercriminal sobrescribir el runC para obtener acceso root y poder ejecutar un comando tanto en nuevos contenedores creados por el atacante como a través de contenedores que ya existen y a los que también tiene acceso.

¿Qué servicios se han visto afectados por esta vulnerabilidad?
Esta vulnerabilidad, catalogada como CVE-2019-5736, ha afectado a los siguientes servicios:

Amazon: se ha comprometido la seguridad de los servicios que incorporan contenedores como ECS, EKS y AWS Fargate del gigante del comercio electrónico. La compañía ha reconocido que esta vulnerabilidad ha afectado a 11 de sus servicios, ha informado a sus clientes de la situación y les ha recomendado que actualicen las últimas versiones.

Google: ha recomendado instalar los últimos parches de seguridad disponibles en los nodos de Ubuntu Kubernetes Engine (GKE) cuyos niveles de seguridad han estado comprometidos

Docker: el proveedor de contenedores Docker ha informado que los productos que cuentan con una versión anterior a 18.09.02 se han visto afectados, pero la propia compañía ha realizado una actualización que incluye un parche de seguridad para combatir esta vulnerabilidad.

Red Hat: el proveedor de soluciones de código abierto también ha sufrido las consecuencias de esta vulnerabilidad; sin embargo, consideran que el número de clientes afectados es bajo.

“La seguridad en la nube sigue siendo una asignatura pendiente para las empresas”, señala Eusebio Nieva, director técnico de Check Point para España y Portugal. Por este motivo, la compañía ha incluido Dome9 en su catálogo de soluciones cloud para mejorar la arquitectura Infinity por medio de políticas activas y protección multi-nube avanzadas. CloudGuard Dome9 detecta el nivel de seguridad utilizando su innovador lenguaje Governance Specification Language (GSL). A diferencia de otros sistemas que requieren escribir códigos para definir reglas, GSL permite crear nuevas reglas escritas en un lenguaje común para facilitar así su comprensión.

“Gracias a CloudGuard Dome9 podemos ayudar a las empresas controlar su estrategia, detectar

errores de configuración y potenciar los puntos fuertes de su estructura de seguridad. De esta forma, podemos alertarles cuando se encuentren expuestas a vulnerabilidades. En el caso de la vulnerabilidad CVE-2019-5736 detectada en Linux, CloudGuard Dome9 puede identificar las vulnerabilidades en los servicios Fargate, y de esta forma reiniciar los servicios con la versión recomendada", señalan desde Check Point.

Datos de contacto:
eVerythink PR

Nota de prensa publicada en: España

Categorías: Internacional Nacional Programación E-Commerce Software Ciberseguridad