Investigadores de seguridad cibernética de Unit 42 de Palo Alto Networks, revelaron los detalles de una nueva vulnerabilidad que afecta a Service Fabric de Microsoft, y que podría explotarse para obtener permisos elevados y tomar el control de todos los nodos en un clúster.

El problema, denominado FabricScape (CVE-2022-30137), podría explotarse en contenedores que están configurados para tener acceso en tiempo de ejecución. Se solucionó el 14 de junio de 2022 en Service Fabric 9.0 Cumulative Update 1.0.

Azure Service Fabric es la plataforma como servicio (PaaS) de Microsoft y una solución orquestadora de contenedores que se utiliza para crear e implementar aplicaciones en la nube basadas en microservicios en un clúster de máquinas.

> *«La vulnerabilidad permite que un mal actor, con acceso a un contenedor comprometido, aumente los privilegios y obtenga el control del nodo SF del host del recurso y todo el clúster. Aunque el error existe en ambas plataformas del sistema operativo, solo se puede explotar en Linux; Windows ha sido examinado minuciosamente y se descubrió que no es vulnerable a este ataque»*, dijo Microsoft como parte del proceso de divulgación coordinado.

Un clúster de Service Fabric es un conjunto conectado a la red de varios nodos (Windows Server o Linux), cada uno de los cuales está diseñado para administrar y ejecutar aplicaciones que constan de microservicios o contenedores.

La vulnerabilidad identificada por Unit 42 reside en un componente llamado Agente de Recopilación de Diagnósticos (DCA) que es responsable de recopilar información de diagnóstico y se relaciona con lo que se denomina una *«carrera de enlace simbólico».*

En un escenario hipotético, un atacante con acceso a una carga de trabajo en contenedores comprometida podría sustituir un archivo leído por el agente («ProcessContainerLog.txt») con un enlace simbólico malicioso que luego podría aprovecharse para sobrescribir cualquier

archivo arbitrario considerando que DCA se ejecuta como root en el nodo.

> *«Si bien este comportamiento se puede observar tanto en los contenedores de Linux como en los contenedores de Windows, solo se puede explotar en los contenedores de Linux porque en los contenedores de Windows, los actores sin privilegios no pueden crear enlaces simbólicos en ese entorno»*, dijo el investigador de Unit42, Aviv Sasson.

Posteriormente, la ejecución del código se logra aprovechando la falla para anular el archivo «/etc/environment» en el host, seguido de la explotación de un trabajo cron interno por hora que se ejecuta como root para importar variables de entorno y maliciosas y cargar un objeto compartido no autorizado en el contenedor comprometido que otorga al atacante un shell inverso en el contexto de root.

> *«Para obtener la ejecución del código, usamos una técnica llamada secuestro dinámico del enlazador. Abusamos de la variable de entorno LD_PRELOAD. Durante la inicialización de un nuevo proceso, en enlazador carga el objeto compartido al que apunta esta variable y, con eso, inyectamos objetos compartidos en los trabajos cron privilegiados en el nodo»,* dijo Sasson.

Aunque no hay evidencia de que la vulnerabilidad haya sido explotada en ataques del mundo real hasta ahora, es crucial que las organizaciones tomen medidas inmediatas para determinar si sus entornos son susceptibles e implementar los parches.