Se han descubierto tres vulnerabilidades graves de seguridad interconectadas en Kubernetes que podrían ser explotadas para lograr la ejecución remota de código con privilegios elevados en dispositivos Windows dentro de un clúster.

Estos problemas, identificados como CVE-2023-3676, CVE-2023-3893 y CVE-2023-3955, tienen una puntuación CVSS de 8.8 y afectan a todos los entornos de Kubernetes que cuentan con nodos Windows. Las correcciones para estas vulnerabilidades se publicaron el 23 de agosto de 2023, después de que Akamai las revelara de manera responsable el 13 de julio de 2023.

> Según el investigador de seguridad de Akamai, Tomer Peled, en un informe técnico, *«esta vulnerabilidad permite la ejecución remota de código con privilegios de SYSTEM en todos los dispositivos Windows dentro de un clúster de Kubernetes. Para explotar esta vulnerabilidad, el atacante debe aplicar un archivo YAML malicioso en el clúster».*

Grandes proveedores de servicios en la nube como Amazon Web Services (AWS), Google Cloud y Microsoft Azure han emitido advertencias sobre estos problemas, los cuales afectan a las siguientes versiones de Kubelet:

- kubelet < v1.28.1
- kubelet < v1.27.5
- kubelet < v1.26.8
- kubelet < v1.25.13
- kubelet < v1.24.17

En resumen, CVE-2023-3676 permite que un atacante con privilegios de «apply» (lo que le permite interactuar con la API de Kubernetes) inyecte código arbitrario que se ejecutará en dispositivos Windows remotos con privilegios de SYSTEM.

> Tomer Peled también señaló que *«CVE-2023-3676 requiere privilegios bajos y, por lo tanto, establece un umbral bajo para los atacantes: lo único que necesitan es acceso a un nodo y privilegios de apply».*

Esta vulnerabilidad, junto con CVE-2023-3955, se produce debido a la falta de saneamiento de la entrada, lo que permite que una cadena de caracteres especialmente diseñada se interprete como un parámetro de un comando PowerShell, lo que conduce a la ejecución de comandos de manera efectiva.

Por otro lado, CVE-2023-3893 se refiere a un caso de escalada de privilegios en la Interfaz de Almacenamiento de Contenedores (CSI) que permite que un actor malicioso obtenga acceso de administrador en el nodo.

> La plataforma de seguridad de Kubernetes, ARMO, destacó el mes pasado que *«un tema común entre estas vulnerabilidades es la falta de saneamiento de entrada en la versión de Kubernetes específica de Windows del Kubelet. Específicamente, cuando se manejan las definiciones de los Pods, el software no valida ni limpia adecuadamente las entradas de los usuarios. Esta omisión permite que los usuarios maliciosos creen Pods con variables de entorno y rutas de host que, cuando se procesan, generan comportamientos no deseados, como la escalada de privilegios».*