Un atacante puede abusar de una vulnerabilidad de seguridad sin parches que afecta a la plataforma Compute Engine de Google, con el fin de hacerse cargo de las máquinas virtuales a través de la red.

> *«Esto sucede haciéndose pasar por el servidor de metadatos desde el punto de vista de la máquina virtual objetivo. Al montar este exploit, el atacante puede otorgarse acceso a sí mismo a través de SSH para luego poder iniciar sesión como usuario root»,* dijo el investigador de seguridad Imre Rad.

Google Compute Engine (GCE) es un componente de infraestructura como servicio (IaaS) de Google Cloud Platform, que permite a los usuarios crear y lanzar máquinas virtuales a pedido. GCE proporciona un método para almacenar y recuperar metadatos en forma de servidor de metadatos, que ofrece un punto central para establecer metadatos en forma de pares clave-valor que luego se proporcionan a las máquinas virtuales en tiempo de ejecución.

Según el investigador, el problema es una consecuencia de números pseudoaleatorios débiles utilizados por el cliente DHCP de ISC, lo que da como resultado un escenario en el que un adversario crea múltiples paquetes DHCP utilizando un conjunto de identificadores de transacciones precalculados (también conocidos como XID) e inunda el DHCP del cliente víctima, lo que en última instancia, conduce a la suplantación del servidor de metadatos.

El Protocolo de Configuración Dinámica de Host (DHCP) es un protocolo de administración de red que se usa para automatizar el proceso de configuración de dispositivos en redes IP. Un servidor DHCP asigna de forma dinámica una dirección IP y otros parámetros de configuración de red a cada dispositivo cliente en una red para que puedan comunicarse con otras redes.

> *«Si el XID es correcto, la máquina víctima aplica la configuración de red. Esta es una condición de carrera, pero debido a que la inundación es rápida y exhaustiva, el servidor de metadatos no tiene ninguna posibilidad real de ganar. En este punto, el*

> *atacante está en la posición de reconfigurar la pila de red de la víctima»,* dijo Rad en su informe técnico.

Debido a que se puede utilizar un servidor de metadatos para distribuir y administrar claves SSH, un cliente, que ahora ha establecido una conexión TCP con el servidor no autorizado, puede recuperar la clave pública SSH del atacante, que luego puede ser utilizada por el atacante para abrir un shell remoto como usuario root.

En un escenario potencial del mundo real, un adversario puede abusar de la cadena de ataques antes mencionada para obtener acceso completo a una máquina virtual objetivo mientras se reinicia o por Internet en los casos en que el firewall de la plataforma en la nube está apagado.

Google fue informado sobre el problema el 27 de septiembre de 2020, fecha desde la que reconoció el informe y lo describió como una *«buena captura»,* pero aún no ha implementado un parche ni ha proporcionado un cronograma de cuándo estará disponible la corrección.

> *«Hasta que llegue la solución, no use DHCP ni configure una regla de firewall a nivel de host para garantizar que la comunicación DHCP provenga del servidor de metadatos (169.254.169.254). Bloquear UDP/68 entre VM, para que solo el servidor de metadatos pueda ejecutar DHCP»*, dijo Rad.

No es la primera vez que Rad identifica problemas con Google Cloud Platform, en septiembre de 2020, Google corrigió una vulnerabilidad de escalada de privilegios local en la herramienta de configuración del sistema operativo, que podría ser aprovechada por un actor con derechos de ejecución de código en las máquinas virtuales de GCE afectadas para realizar operaciones no autorizadas.

Después, a inicios de enero, Rad también descubrió que era posible lograr la ejecución de código arbitrario en una máquina virtual al obtener un shell en el servicio de base de datos

de Cloud SQL. Google abordó el problema el 16 de febrero de 2021.