Los investigadores en ciberseguridad han revelado una vulnerabilidad de escalada de privilegios que afecta al servicio Cloud Functions de Google Cloud Platform, la cual podría ser aprovechada por un atacante para acceder a otros servicios y datos sensibles de manera no autorizada.

Tenable ha bautizado esta vulnerabilidad como ConfusedFunction.

> *«Un atacante podría elevar sus privilegios a la cuenta de servicio predeterminada de Cloud Build y acceder a numerosos servicios como Cloud Build, almacenamiento (incluido el código fuente de otras funciones), registro de artefactos y registro de contenedores»,* afirmó la empresa de gestión de exposiciones en un comunicado.
>
> *«Este acceso permite el movimiento lateral y la escalada de privilegios en el proyecto de una víctima, para acceder a datos no autorizados e incluso actualizarlos o eliminarlos.»*

Cloud Functions es un entorno de ejecución sin servidor que permite a los desarrolladores crear funciones de propósito único que se activan en respuesta a eventos específicos en la nube, sin necesidad de gestionar un servidor o actualizar frameworks.

El problema descubierto por Tenable radica en el hecho de que una cuenta de servicio de Cloud Build se crea en segundo plano y se vincula a una instancia de Cloud Build de forma predeterminada cuando se crea o actualiza una función en la nube.

Esta cuenta de servicio ofrece la posibilidad de realizar actividades maliciosas debido a sus permisos excesivos, permitiendo así que un atacante con acceso pueda crear o actualizar una función en la nube y aprovechar esta vulnerabilidad para elevar sus privilegios a la cuenta de servicio.

Estos permisos podrían ser explotados para acceder a otros servicios de Google Cloud que

también se crean junto con la función en la nube, como Cloud Storage, Artifact Registry y Container Registry. En un escenario de ataque hipotético, ConfusedFunction podría ser utilizada para filtrar el token de la cuenta de servicio de Cloud Build a través de un webhook.

Tras una divulgación responsable, Google ha actualizado el comportamiento predeterminado para que Cloud Build utilice la cuenta de servicio predeterminada de Compute Engine y así prevenir su mal uso. Sin embargo, es importante destacar que estos cambios no se aplican a las instancias existentes.

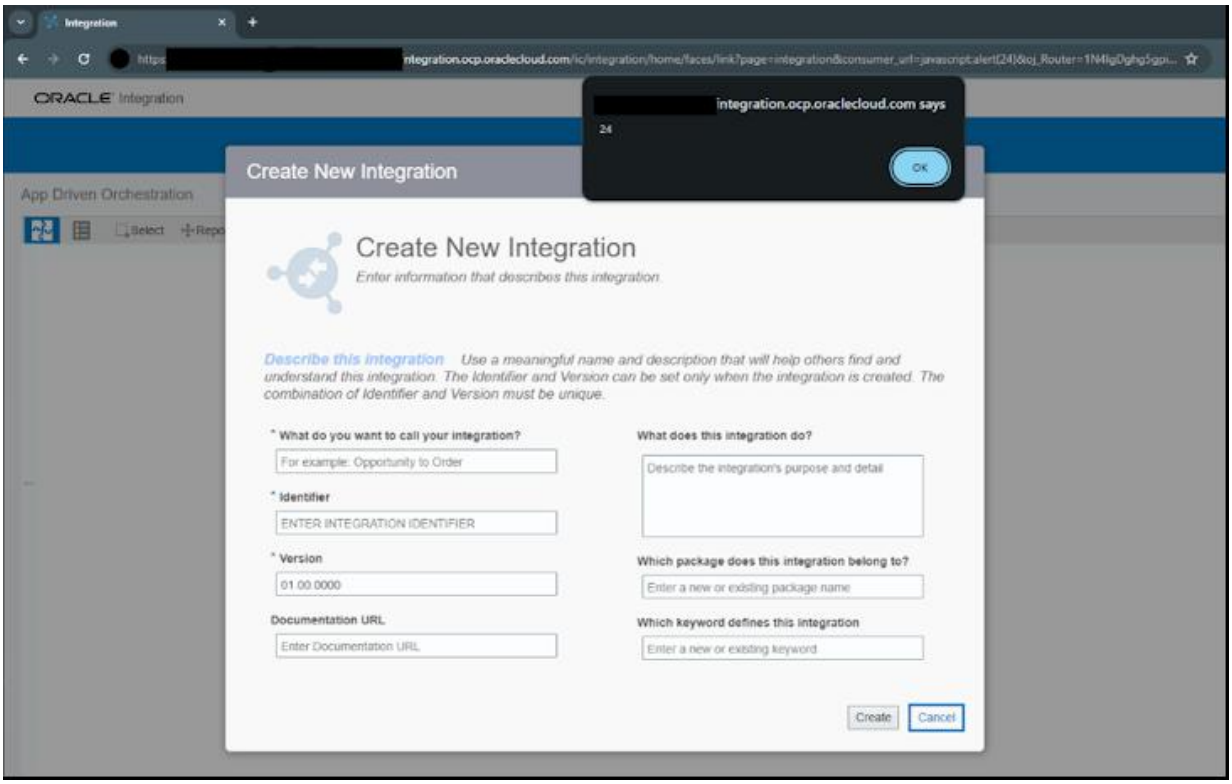
> *«La vulnerabilidad ConfusedFunction pone de manifiesto los escenarios problemáticos que pueden surgir debido a la complejidad del software y la comunicación entre servicios en los servicios de un proveedor de nube»,* señaló el investigador de Tenable, Liv Matan.
>
> *«Aunque la solución de GCP ha reducido la gravedad del problema para futuros despliegues, no lo ha eliminado por completo. Esto se debe a que el despliegue de una función en la nube sigue desencadenando la creación de los servicios de GCP mencionados anteriormente. Como resultado, los usuarios aún deben asignar permisos mínimos pero relativamente amplios a la cuenta de servicio de Cloud Build como parte del despliegue de una función.»*

Este desarrollo se produce cuando Outpost24 detalló una vulnerabilidad de severidad media de cross-site scripting (XSS) en la plataforma Oracle Integration Cloud que podría ser explotada para inyectar código malicioso en la aplicación.

La vulnerabilidad, que reside en el manejo del parámetro «*consumer_url*«, fue resuelta por Oracle en su Actualización Crítica de Parches (CPU) lanzada a principios de este mes.

> *«La página para crear una nueva integración, encontrada en*

> *https://.integration.ocp.oraclecloud.com/ic/integration/home/faces/link?page=integration&consumer_url=, no requería ningún otro parámetro»*, explicó el investigador de seguridad Filip Nyquist.



> *«Esto significaba que un atacante solo necesitaría identificar el instance-id de la plataforma de integración específica para enviar una carga útil funcional a cualquier usuario de la plataforma. En consecuencia, el atacante podría eludir el requisito de conocer una ID de integración específica, que típicamente es accesible solo para usuarios registrados.»*

Esto también se produce después del descubrimiento de Assetnote de tres vulnerabilidades de seguridad en la plataforma de computación en la nube ServiceNow (CVE-2024-4879, CVE-2024-5178 y CVE-2024-5217) que podrían ser combinadas en una cadena de

explotación para obtener acceso completo a la base de datos y ejecutar código arbitrario en el contexto de la Now Platform.