Investigadores de seguridad cibernética revelaron hoy los detalles de una nueva vulnerabilidad en la plataforma VMware´s Cloud Director, que podría permitir a un hacker obtener acceso a información confidencial y controlar nubes privadas dentro de una infraestructura completa.

Identificada como CVE-2020-3956, la vulnerabilidad de inyección de código se deriva de un manejo de entrada incorrecto que podría ser abusado por un atacante autenticado para enviar tráfico malicioso a Cloud Director, lo que podría llevar a la ejecución de código arbitrario.

La vulnerabilidad está clasificada en 8.8 de 10, en escala de gravedad CVSS v.3, por lo que se trata de una vulnerabilidad crítica.

VMware Cloud Director es un popular software de implementación, automatización y administración que se utiliza para operar y administrar recursos en la nube, lo que permite a las empresas y centros de datos distribuirse en distintas partes del mundo en centros de datos virtuales.

Según la compañía, la vulnerabilidad puede explotarse a través de las interfaces de usuario basadas en HTML5 y Flex, la interfaz API Explorer y el acceso a la API.

La vulnerabilidad afecta a las versiones de VMware Cloud Director 10.0.x antes de 10.0.0.2, 9.7.0.x antes de 9.7.0.5, 9.5.0.x antes de 9.5.0.6 y 9.1.0.x antes de 9.1.0.4.

La vulnerabilidad fue identificada por una empresa de piratería ética con sede en Praga, Citadelo, luego de ser contratada a inicios del año por un cliente empresarial no identificado de Fortune 500, para llevar a cabo una auditoría de seguridad de su infraestructura en la nube. La empresa publicó una prueba de concepto para demostrar la gravedad del exploit.

> *«Todo comenzó con una simple anomalía. Cuando ingresamos ${7*7} como nombre de host para el servidor SMPT en vCloud Director, recibimos el siguiente*

> *mensaje de error: El valor de la cadena tiene un valor no válido, valor [49]. Indicaba alguna forma de inyección de lenguaje de expresión, ya que pudimos evaluar funciones aritméticas simples en el lado del servidor»*, dijo Citadelo.

Con esto como punto de entrada, los investigadores dijeron que podían acceder a clases arbitrarias de Java (por ejemplo, «java.io.BufferedReader») y crear instancias al pasar cargas maliciosas.

Citadelo dijo que pudo realizar el siguiente conjunto de acciones al explotar la falla:

- Ver el contenido de la base de datos del sistema interno, incluidos los valores hash de contraseña de los clientes asignados a la infraestructura.
- Modificar la base de datos del sistema para acceder a máquinas virtuales extranjeras (VM) asignadas a diferentes organizaciones dentro de Cloud Director.
- Escalar los privilegios de «Administrador de la organización» a «Administrador del sistema» con acceso a todas las cuentas en la nube simplemente cambiando la contraseña por medio de una consulta SQL.
- Modificar la página de inicio de sesión de Cloud Director, permitiendo que el atacante capture las contraseñas de otro cliente en texto plano, incluyendo las cuentas de administrador del sistema.
- Leer otros datos confidenciales relacionados con los clientes, como nombres completos, direcciones de correo electrónico o direcciones IP.

Después de que Citadelo revelara en privado los hallazgos a VMware el pasado 1 de abril, la compañía corrigió los defectos en una serie de actualizaciones que abarcan las versiones 9.1.0.4, 9.5.0.6, 9.7.0.5 y 10.0.0.2.

VMware también lanzó una solución alternativa para mitigar el riesgo de ataques que exploten el problema.

> *«En general, la infraestructura de la nube se considera relativamente segura porque*

> *se están implementando distintas capas de seguridad dentro de su núcleo, como el cifrado, el aislamiento del tráfico de red o la segmentación de clientes. Sin embargo, se pueden encontrar vulnerabilidades de seguridad en cualquier tipo de aplicación, incluida la nube de proveedores»*, dijo Tomas Zatko, CEO de Citadelo.