La compañía de tecnología de computación en la nube y virtualización VMware lanzó el jueves pasado una actualización que tiene como finalidad corregir una vulnerabilidad de seguridad crítica en su producto Cloud Director, que podría utilizarse como arma para lanzar ataques de ejecución remota de código.

La vulnerabilidad, rastreada como CVE-2022-22966, tiene una puntuación CVSS de 9.1. VMware brindó el crédito al investigador de seguridad Jari Jääskelä por informar sobre la falla.

> *«Un actor malicioso autenticado y con muchos privilegios con acceso a la red del inquilino o proveedor de VMware Cloud Director puede explotar una vulnerabilidad de ejecución remota de código para obtener acceso al servidor»,* dijo VMware.

VMware Cloud Director, antes conocido como vCloud Director, se utiliza por muchos proveedores de nube conocidos para operar y administrar sus infraestructuras de nube y obtener visibilidad de los centros de datos en todos los sitios y geografías.

La vulnerabilidad podría terminar permitiendo que los atacantes obtengan acceso a datos confidenciales y se apoderen de nubes privadas dentro de una infraestructura completa.

Las versiones afectadas incluyen 10.1.x, 10.2.x y 10.3.x, con correcciones disponibles en las versiones 10.1.4.1, 10.2.2.3 y 10.3.3. La compañía también publicó soluciones alternativas que se pueden seguir cuando la actualización a una versión recomendada no es una opción.

Los parches llegan un día después de que se detectaran vulnerabilidades para otra vulnerabilidad crítica recientemente corregida en VMware Workspace ONE Access.

La falla CVE-2022-22954 se relaciona con una vulnerabilidad de ejecución remota de código que se deriva de la inyección de plantillas del lado del servidor en VMware Workspace ONE Access e Identity Manager.

Debido a que los productos de VMware por lo general se convierten en objetivo lucrativo para

los actores de amenazas, la actualización se suma a la urgencia de que las organizaciones apliquen las mitigaciones necesarias para prevenir amenazas potenciales.