Una vulnerabilidad crítica en el dispositivo VMware Carbon Black Cloud Workload, podría aprovechare para evitar la autenticación y tomar el control de los sistemas vulnerables.

Rastreada como CVE-2021-21982, la vulnerabilidad tiene una calificación de 9.1 de una máximo de 10 en el sistema de puntuación CVSS, y afecta a todas las versiones del producto anteriores a la 1.0.1.

Carbon Black Cloud Workload es un producto de seguridad para centros de datos de VMware, que tiene como objetivo proteger los servidores críticos y las cargas de trabajo alojadas en vSphere, la plataforma de virtualización de computación en la nube de la compañía.

> *«Una URL en la interfaz administrativa del dispositivo VMware Carbon Black Cloud Workload puede manipularse para evitar la autenticación»,* dijo VMware en su aviso.

Esto permite que un adversario con acceso de red a la interfaz obtenga acceso a la API de administración del dispositivo. Armado con el acceso, un actor malintencionado puede ver y alterar la configuración administrativa.

Además de lanzar una solución para CVE-2021-21982, VMware también abordó dos errores separados en su solución vRealize Operations Manager, que un atacante con acceso de red a la API podría aprovechar para llevar a cabo ataques de falsificación de solicitudes del lado del servidor (SSRF) para robar credenciales administrativas (CVE-2021-21975) y escribir archivos en ubicaciones arbitrarias en el sistema operativo de fotones subyacente (CVE-2021-21983).

El producto está diseñado principalmente para monitorear y optimizar el rendimiento de la infraestructura virtual y funciones de soporte como el equilibrio de la carga de trabajo, la resolución de problemas y la gestión del cumplimiento.

Egor Dimitrenko, investigador de seguridad de Positive Technologies, fue quien informó sobre las tres vulnerabilidades.

> *«El principal riesgo es que los privilegios de administrador permiten a los atacantes explotar la segunda vulnerabilidad: CVE-2021-21983 (una falla de escritura de archivo arbitraria, puntuada con 7.2), que permite ejecutar cualquier comando en el servidor. La combinación de dos fallas de seguridad hace que la situación sea aún más peligrosa, ya que permite que un atacante no autorizado obtenga el control del servidor y se mueva lateralmente dentro de la infraestructura»*, dijo Dimitrenko.

VMware lanzó parches para las versiones 7.0.0, 7.5.0, 8.0.1, 8.1.1, 8.2.0 y 8.3.0 de vRealize Operations Manager. La compañía también publicó soluciones para mitigar los riesgos asociados con las fallas en escenarios donde el parche no se puede instalar o no se encuentra disponible.