Un grupo de piratas informáticos han estado escaneando activamente Internet en busca de servidores VMware vCenter vulnerables, que no estén parcheados contra una falla crítica de ejecución remota de código, misma que la compañía abordó a fines de mayo.

La actividad en curso fue detectada por Bad Packets el 3 de junio, y corroborada este viernes por el investigador de seguridad, Kevin Beaumont.

> *«Se detectó actividad de escaneo masivo desde 104.40.252.159 al verificar hosts VMware vSphere vulnerables a la ejecución remota de código»*, dijo Troy Mursch, director de investigación de Bad Packets.

El desarrollo sigue a la publicación de un código de explotación RCE de prueba de concepto (PoC) dirigido al error de VMware vCenter.

Registrado como CVE-2021-21985 con puntuación CVSS de 9.8, el problema es una consecuencia de la falta de validación de entrada en el complemento de comprobación de estado de Virtual San (vSAN), que un atacante podría abusar para realizar ejecución de comandos con privilegios ilimitados en el sistema operativo subyacente que aloja vCenter Server.

Aunque VMware corrigió la falla el 25 de mayo, la compañía instó encarecidamente a sus clientes a aplicar el cambio de emergencia inmediatamente.

> *«En esta era de ransomware, es más seguro asumir que un atacante ya está dentro de la red en algún lugar, en un escritorio y tal vez incluso en el control de una cuenta de usuario, por lo que recomendamos encarecidamente declarar un cambio de emergencia y parchear lo antes posible»,* dijo VMware.

Esta no es la primera vez que los atacantes escanean masivamente Internet de forma

oportunista en busca de servidores VMware vCenter vulnerables. Una vulnerabilidad de ejecución remota de código similar (CVE-2021-21972) que fue parcheada por VMware en febrero, se convirtió en el objetivo de los actores de amenazas cibernéticas que intentan explotar y tomar el control de los sistemas no parcheados.

Se encontraron al menos 14,858 servidores vCenter accesibles a través de Internet, según Bad Packets y Binary Edge.

Además, una nueva investigación de Cisco Talos a inicios de esta semana, descubrió que el actor de amenazas detrás del bot Necro basado en Python, se abrió camino hasta los servidores VMware vCenter expuestos al abusar de la misma debilidad de seguridad para aumentar las capacidades de propagación de infecciones de malware.