Se ha observado que un atacante relacionado con Irán, conocido como Rocket Kitten, explota activamente una vulnerabilidad de VMware parcheada recientemente para obtener acceso inicial e implementar la herramienta de prueba de penetración Core Impact en sistemas vulnerables.

Rastreada como CVE-2022-22954, con puntuación CVSS de 9.8, la vulnerabilidad crítica se refiere a un caso de ejecución remota de código que afecta a VMware Workspace ONE Access e Identity Manager.

Aunque la vulnerabilidad fue corregida por el proveedor de servicios de virtualización el 6 de abril de 2022, la compañía advirtió a los usuarios sobre la explotación confirmada de la falla que ocurre en la naturaleza una semana después.

> *«Un actor malicioso que explote esta vulnerabilidad RCE obtiene potencialmente una superficie de ataque ilimitada. Esto significa el acceso privilegiado más alto a cualquier componente del entorno virtualizado de host e invitado»,* dijeron los investigadores de Morphisec.

Las cadenas de ataque que explotan la vulnerabilidad implican la distribución de un controlador de etapas basado en PowerShell, que luego se utiliza para descargar una carga útil de siguiente etapa llamada PowerTrash Loader que, a su vez, inyecta la herramienta de prueba de penetración Core Impact en la memoria para actividades de seguimiento.

> *«El uso generalizado de la administración de acceso a la identidad de VMware combinado con el acceso remoto sin restricciones que proporciona este ataque es una receta para brechas devastadoras en todas las industrias»,* dijeron los investigadores.

> *«Los clientes de VMware también deben revisar su arquitectura de VMware para asegurarse de que los componentes afectados no se publiquen accidentalmente en Internet, lo que aumenta drásticamente los riesgos de explotación»*, agregaron.