Los actores de amenazas presuntamente están explotando una falla de seguridad de gravedad máxima que afecta a Quest KACE Systems Management Appliance (SMA), según Arctic Wolf.

La empresa de ciberseguridad indicó que observó actividad maliciosa a partir de la semana del 9 de marzo de 2026 en entornos de clientes, la cual coincide con la explotación de CVE-2025-32975 en sistemas SMA sin parches expuestos a internet. Por el momento, se desconocen los objetivos finales del ataque.

CVE-2025-32975 (puntuación CVSS: 10.0) se refiere a una vulnerabilidad de omisión de autenticación que permite a los atacantes hacerse pasar por usuarios legítimos sin credenciales válidas. La explotación exitosa de esta falla podría permitir la toma total de cuentas administrativas. El problema fue corregido por Quest en mayo de 2025.

En la actividad maliciosa detectada por Arctic Wolf, se cree que los actores de amenazas han aprovechado esta vulnerabilidad para apoderarse de cuentas administrativas y ejecutar comandos remotos con el fin de descargar cargas útiles codificadas en Base64 desde un servidor externo (216.126.225[.]156) mediante el comando curl.

Los atacantes, cuya identidad se desconoce, posteriormente procedieron a crear cuentas administrativas adicionales a través de «*runkbot.exe*«, un proceso en segundo plano asociado con el agente SMA que se utiliza para ejecutar scripts y gestionar instalaciones. También se detectaron modificaciones en el Registro de Windows mediante un script de PowerShell, posiblemente para mantener persistencia o alterar la configuración del sistema.

Otras acciones llevadas a cabo por los actores de amenazas incluyen:

- Realización de robo de credenciales utilizando Mimikatz.
- Ejecución de tareas de descubrimiento y reconocimiento mediante la enumeración de usuarios conectados y cuentas administrativas, así como la ejecución de los comandos *«net time»* y *«net group»*.
- Obtención de acceso mediante protocolo de escritorio remoto (RDP) a infraestructuras

de respaldo (Veeam, Veritas) y controladores de dominio.

Para mitigar la amenaza, se recomienda a los administradores aplicar las actualizaciones más recientes y evitar exponer instancias de SMA a internet. El problema ha sido solucionado en las versiones 13.0.385, 13.1.81, 13.2.183, 14.0.341 (Parche 5) y 14.1.101 (Parche 4).