Los grupos de ransomware INC y Qilin están explotando una vulnerabilidad de Palo Alto Networks para eludir la autenticación multifactor

Palo Alto Networks informó que continúa detectando la explotación de una vulnerabilidad de seguridad, ya corregida, que afecta a PAN-OS y Prisma Access y que está siendo aprovechada por grupos dedicados a la distribución de ransomware.

La actividad está relacionada con la vulnerabilidad CVE-2026-0257, que cuenta con una puntuación CVSS de 7.8. Se trata de una falla que permite eludir los mecanismos de autenticación y que los actores maliciosos podrían utilizar para establecer conexiones VPN sin autorización. Palo Alto Networks publicó una corrección en mayo de 2026, mientras que la Agencia de Ciberseguridad y Seguridad de las Infraestructuras de Estados Unidos (CISA) incorporó la vulnerabilidad a su catálogo de vulnerabilidades explotadas conocidas (Known Exploited Vulnerabilities, KEV) el 13 de mayo de 2026.

«Entre los operadores de ransomware que explotan la vulnerabilidad CVE-2026-0257 se encuentran Spikey Scorpius (también conocido como Qilin) y Tarnished Scorpius (también conocido como INC)», señalaron los investigadores de Unit 42 en una actualización publicada el lunes. Este anuncio se produjo pocos días después de que ReliaQuest informara sobre la detección de los grupos de ransomware Qilin y Settra, que estaban aprovechando activamente esta vulnerabilidad para llevar a cabo ataques con motivaciones económicas.

De acuerdo con Unit 42, los actores de amenazas utilizan esta falla para obtener un punto de acceso inicial a las redes corporativas y, posteriormente, evadir los controles de autenticación multifactor (MFA) con el objetivo de establecer una sesión VPN.

Una vez que consiguen establecer la conexión VPN, los atacantes han sido observados realizando diversas actividades posteriores al compromiso, entre ellas:

- Examinar la red interna mediante herramientas de supervisión y administración remota (Remote Monitoring and Management, RMM) que pueden utilizarse tanto con fines legítimos como maliciosos.
- Desplazarse lateralmente por la infraestructura de red mediante los protocolos RDP y SMB.
- Preparar herramientas adicionales destinadas al robo de credenciales, la extracción de

información y la implementación de ransomware.

Según los informes, los ataques perpetrados por estos grupos han afectado a organizaciones de numerosos sectores, incluidos educación, servicios financieros, atención sanitaria, alta tecnología, hotelería, manufactura, servicios profesionales y jurídicos, gobierno, transporte y logística, servicios públicos y energía, así como comercio minorista.

«El cambio más relevante en las tácticas, técnicas y procedimientos (TTP) después de explotar con éxito la vulnerabilidad CVE-2026-0257 consiste en pasar directamente a la capa de virtualización», indicó Unit 42.

«En un caso destacado, los atacantes se desplazaron desde la puerta de enlace VPN comprometida hasta el dispositivo de administración de vCenter. Desde allí, desactivaron controles de seguridad en los hipervisores ESXi (execInstalledOnly) y utilizaron una herramienta personalizada para extraer credenciales sin conexión directamente del disco virtual (VMDK) de un controlador de dominio».

La empresa especializada en seguridad de redes añadió que esta técnica permite eludir los mecanismos de detección y respuesta en los equipos (Endpoint Detection and Response, EDR), así como otras protecciones implementadas dentro de los sistemas operativos invitados. Esto facilita que los atacantes obtengan credenciales con alcance sobre todo el dominio.

También se ha observado que los responsables de estos ataques combinan el método de acceso inicial con otras herramientas de explotación. Entre sus objetivos se encuentra la infraestructura de copias de seguridad de Veeam, contra la cual aprovechan vulnerabilidades conocidas, como CVE-2023-27532, para maximizar el impacto de sus operaciones.

Cabe señalar que Arctic Wolf ya había advertido sobre la explotación de CVE-2026-0257 por parte del grupo Qilin en julio de 2026. Las actividades detectadas abarcaron desde ataques rápidos centrados exclusivamente en cifrar archivos hasta operaciones de doble extorsión, en las que los atacantes cifran los datos y amenazan con divulgar la información robada.

Además de instalar las actualizaciones de seguridad más recientes, Palo Alto Networks recomienda que las organizaciones busquen de forma proactiva indicadores de compromiso y activen los procedimientos de respuesta a incidentes correspondientes cuando detecten eventos que indiquen una posible conexión exitosa a través de una puerta de enlace comprometida.