Una vulnerabilidad de seguridad de gravedad máxima en Dell RecoverPoint for Virtual Machines ha sido explotada como zero-day por un presunto grupo vinculado a China identificado como UNC6201 desde mediados de 2024, según un nuevo informe de Google Mandiant y Google Threat Intelligence Group (GTIG).

La actividad implica la explotación de CVE-2026-22769 (CVSS: 10.0), una falla relacionada con credenciales codificadas de forma rígida que afecta a versiones anteriores a 6.0.3.1 HF1. Otros productos, como RecoverPoint Classic, no se ven afectados.

«Se considera crítica porque un atacante remoto no autenticado que conozca la credencial integrada podría explotar esta vulnerabilidad, lo que derivaría en acceso no autorizado al sistema operativo subyacente y persistencia con privilegios de root», indicó Dell en un boletín publicado el martes.

El problema impacta a los siguientes productos:

- RecoverPoint for Virtual Machines versión 5.3 SP4 P1 – Migrar desde la versión 5.3 SP4 P1 a 6.0 SP3 y posteriormente actualizar a 6.0.3.1 HF1
- RecoverPoint for Virtual Machines versiones 6.0, 6.0 SP1, 6.0 SP1 P1, 6.0 SP1 P2, 6.0 SP2, 6.0 SP2 P1, 6.0 SP3 y 6.0 SP3 P1 – Actualizar a 6.0.3.1 HF1
- RecoverPoint for Virtual Machines versiones 5.3 SP4, 5.3 SP3, 5.3 SP2 y anteriores – Actualizar primero a 5.3 SP4 P1 o a una versión 6.x y luego aplicar la corrección correspondiente

«Dell recomienda que RecoverPoint for Virtual Machines se implemente dentro de una red interna confiable y con controles de acceso, protegida por firewalls adecuados y segmentación de red», señaló la compañía. «RecoverPoint for Virtual Machines no está diseñado para utilizarse en redes públicas o no confiables.»

Según Google, la credencial incrustada corresponde a un usuario “admin” de la instancia Apache Tomcat Manager, lo que permitiría autenticarse en el administrador Tomcat de Dell RecoverPoint, cargar una web shell denominada SLAYSTYLE mediante el endpoint

«/manager/text/deploy» y ejecutar comandos como root en el dispositivo para desplegar la puerta trasera BRICKSTORM y su versión más reciente llamada GRIMBOLT.

«Se trata de una puerta trasera en C# compilada mediante compilación nativa anticipada (AOT), lo que dificulta su ingeniería inversa», añadió Charles Carmakal, de Mandiant.

Google indicó que la actividad ha afectado a organizaciones en Norteamérica, y que GRIMBOLT incorpora mejoras para evadir la detección y reducir rastros forenses en los sistemas comprometidos. *«GRIMBOLT se integra aún mejor con los archivos nativos del sistema», añadió.*

También se considera que UNC6201 presenta similitudes con UNC5221, otro grupo de espionaje vinculado a China conocido por explotar tecnologías de virtualización y vulnerabilidades zero-day en Ivanti para distribuir web shells y malware como BEEFLUSH, BRICKSTORM y ZIPLINE.

Pese a las coincidencias tácticas, actualmente se evalúa que ambos clústeres son distintos. Cabe señalar que el uso de BRICKSTORM también fue atribuido por CrowdStrike a un tercer actor alineado con China denominado Warp Panda, en ataques dirigidos contra entidades estadounidenses.

Un aspecto destacado de la campaña reciente es la utilización por parte de UNC6201 de interfaces de red virtuales temporales —conocidas como “Ghost NICs”— para pivotar desde máquinas virtuales comprometidas hacia entornos internos o SaaS, eliminándolas posteriormente para borrar evidencias y dificultar las investigaciones.

«En línea con la campaña anterior de BRICKSTORM, UNC6201 continúa atacando dispositivos que normalmente no cuentan con agentes tradicionales de detección y respuesta en endpoints (EDR), lo que les permite permanecer sin ser detectados durante largos periodos», señaló Google.

Aún no está claro cómo obtienen el acceso inicial, aunque, al igual que UNC5221, se sabe

que apuntan a dispositivos perimetrales para infiltrarse en redes objetivo. El análisis de dispositivos VMware vCenter comprometidos reveló además comandos iptables ejecutados mediante la web shell para:

- Supervisar tráfico entrante en el puerto 443 en busca de una cadena HEX específica
- Añadir la IP de origen detectada a una lista y permitir la conexión al puerto 10443 si dicha IP figura en la lista
- Redirigir silenciosamente el tráfico posterior del puerto 443 al 10443 durante 300 segundos (cinco minutos) si la IP está autorizada

Asimismo, en septiembre de 2025, el actor reemplazó antiguos binarios de BRICKSTORM por GRIMBOLT. Aunque este último también ofrece acceso remoto tipo shell y emplea el mismo servidor de comando y control (C2), no está claro si el cambio respondió a una estrategia planificada o a la divulgación pública sobre BRICKSTORM.

«Los actores patrocinados por estados continúan apuntando a sistemas que normalmente no admiten soluciones EDR, lo que dificulta enormemente que las organizaciones detecten que han sido comprometidas y prolonga considerablemente el tiempo de permanencia de la intrusión», afirmó Carmakal.

La divulgación coincide con una advertencia de Dragos sobre ataques de grupos chinos como Volt Typhoon (también conocido como Voltzite), orientados a comprometer pasarelas Sierra Wireless Airlink en los sectores eléctrico y de petróleo y gas, para luego pivotar hacia estaciones de trabajo de ingeniería y extraer configuraciones y datos de alarmas.

La actividad, según la firma de ciberseguridad, ocurrió en julio de 2025. Se indica que el acceso inicial fue obtenido a través de Sylvanite, que explota rápidamente vulnerabilidades en dispositivos perimetrales antes de que se apliquen parches y posteriormente transfiere el acceso para intrusiones más profundas en tecnología operativa (OT).

«Voltzite fue más allá de la simple exfiltración de datos y pasó a manipular directamente estaciones de trabajo de ingeniería para analizar qué podría provocar la detención de

procesos», señaló Dragos. «Esto elimina la última barrera práctica entre tener acceso y generar consecuencias físicas. Las pasarelas celulares crean vías no autorizadas hacia redes OT, eludiendo los controles de seguridad tradicionales.»