La Agencia de Seguridad de Infraestructura y Ciberseguridad de los Estados Unidos (CISA) informó el jueves que Commvault está rastreando actividades cibernéticas maliciosas dirigidas a aplicaciones alojadas en su entorno en la nube de Microsoft Azure.

> *"Los actores de amenazas podrían haber obtenido acceso a secretos de clientes vinculados con la solución de respaldo como servicio (SaaS) de Microsoft 365 (M365) de Commvault (Metallic), alojada en Azure",* indicó la agencia.
>
> *"Esto permitió a los actores de amenazas acceder sin autorización a los entornos M365 de clientes de Commvault que almacenan secretos de aplicaciones gestionados por Commvault."*

CISA también señaló que esta actividad podría formar parte de una operación más amplia que busca comprometer infraestructuras en la nube de diversos proveedores de servicios SaaS, especialmente aquellas con configuraciones predeterminadas y permisos excesivos.

Este comunicado se emite pocas semanas después de que Commvault informara que Microsoft notificó a la empresa, en febrero de 2025, sobre una intrusión no autorizada de un actor estatal en su entorno de Azure.

La investigación del incidente reveló que los atacantes aprovecharon una vulnerabilidad no divulgada (CVE-2025-3928) en el servidor web de Commvault, lo que les permitió ejecutar comandos de forma remota a través de web shells tras autenticarse.

> *"Según expertos del sector, este actor de amenazas emplea técnicas avanzadas para intentar obtener acceso a los entornos M365 de los clientes. Este actor podría haber accedido a un subconjunto de credenciales de aplicaciones utilizadas por ciertos clientes de Commvault para autenticar sus entornos M365″,* explicó Commvault en un comunicado.

Commvault aseguró que ha implementado varias medidas correctivas, incluyendo la rotación de credenciales de aplicaciones para M365, y destacó que no se ha detectado acceso no autorizado a los datos de respaldo de los clientes.

Para reducir el riesgo de este tipo de amenazas, CISA recomienda a usuarios y administradores seguir las siguientes pautas:

- Supervisar los registros de auditoría de Entra para detectar modificaciones o adiciones no autorizadas de credenciales en los principales servicios iniciados por aplicaciones o entidades de Commvault
- Revisar los registros de Microsoft (auditoría de Entra, inicios de sesión de Entra, registros de auditoría unificada) y llevar a cabo búsquedas internas de amenazas
- En el caso de aplicaciones de un solo inquilino, establecer políticas de acceso condicional que restrinjan la autenticación del principal de servicio a direcciones IP aprobadas dentro del rango de direcciones permitidas de Commvault
- Verificar las aplicaciones registradas y los principales de servicio en Entra que tengan consentimiento administrativo para privilegios superiores a los necesarios
- Limitar el acceso a las interfaces de administración de Commvault solo a redes y sistemas administrativos confiables
- Implementar un firewall de aplicaciones web para bloquear intentos de recorrido de directorios y cargas sospechosas, y eliminar el acceso externo a aplicaciones de Commvault

CISA, que incluyó la vulnerabilidad CVE-2025-3928 en su Catálogo de Vulnerabilidades Conocidas y Explotadas a finales de abril de 2025, indicó que continúa investigando la actividad maliciosa en conjunto con organizaciones colaboradoras.