Commvault ha publicado actualizaciones para corregir cuatro fallas de seguridad que podrían ser aprovechadas para ejecutar código de manera remota en instancias vulnerables.

La lista de vulnerabilidades, presentes en versiones de Commvault anteriores a la 11.36.60, es la siguiente:

- *CVE-2025-57788 (puntaje CVSS: 6.9)* – Una debilidad en un mecanismo de autenticación conocido permite que atacantes no autenticados realicen llamadas a la API sin necesidad de credenciales de usuario.
- *CVE-2025-57789 (puntaje CVSS: 5.3)* – Una falla durante la fase de configuración, entre la instalación y el primer inicio de sesión del administrador, posibilita que atacantes remotos aprovechen las credenciales predeterminadas para obtener control administrativo.
- *CVE-2025-57790 (puntaje CVSS: 8.7)* – Una vulnerabilidad de *path traversal* que habilita a atacantes remotos a acceder de forma no autorizada al sistema de archivos mediante esta técnica, lo que deriva en ejecución remota de código.
- *CVE-2025-57791 (puntaje CVSS: 6.9)* – Una deficiencia que permite a atacantes externos inyectar o alterar parámetros de línea de comandos enviados a componentes internos, debido a una validación insuficiente de entradas, lo que resulta en el inicio de sesión válido de un usuario con bajos privilegios.

Los investigadores *Sonny Macdonald* y *Piotr Bazydlo* de *watchTowr Labs* han sido reconocidos por descubrir y reportar estos cuatro fallos de seguridad en abril de 2025. Todas las vulnerabilidades señaladas fueron solucionadas en las versiones 11.32.102 y 11.36.60. La solución SaaS de Commvault no se ve afectada.

En un análisis publicado el miércoles, la compañía de ciberseguridad señaló que actores maliciosos podrían encadenar estas vulnerabilidades en dos rutas de explotación previas a la autenticación para lograr ejecución de código en instancias afectadas: una que combina *CVE-2025-57791* con *CVE-2025-57790*, y otra que enlaza *CVE-2025-57788*, *CVE-2025-57789* y *CVE-2025-57790*.

Cabe destacar que la segunda cadena de explotación remota solo tiene éxito si la contraseña de administrador predeterminada no ha sido modificada desde la instalación.

Esta revelación llega casi cuatro meses después de que *watchTowr Labs* informara sobre una vulnerabilidad crítica en el *Commvault Command Center* (*CVE-2025-34028, puntaje CVSS: 10.0*) que permitía la ejecución arbitraria de código en instalaciones afectadas.

Un mes más tarde, la *Agencia de Ciberseguridad y Seguridad de Infraestructura de EE. UU. (CISA)* incorporó la vulnerabilidad en su catálogo de *Known Exploited Vulnerabilities (KEV)*, tras contar con evidencia de explotación activa en entornos reales.