В программном обеспечении Commvault Command Center обнаружена уязвимость максимальной степени опасности (CVE-2025-34028), позволяющая хакерам выполнять произвольный код без аутентификации, сообщает Dark Reading.

Уязвимость, найденная исследователями watchTowr, затрагивает версии 11.38.0–11.38.19 и связана с серверной подделкой запросов (SSRF). Это позволяет злоумышленникам отправлять несанкционированные запросы к внутренним или внешним системам, получая доступ к критически важным данным и системам резервного копирования.

Commvault оперативно выпустила патч (версия 11.38.20), но эксперты подчёркивают: уязвимость особенно опасна из-за привилегированного доступа, который Commvault имеет в корпоративных сетях. «Успешная атака может привести к утечке данных, шифрованию резервных копий или полному контролю над восстановлением», — отметил Эрик Шваке из Salt Security. Хит Ренфроу из Fenix24 советует срочно ограничить интернет-доступ к интерфейсу Command Center до применения обновления.

Организациям рекомендовано проверить настройки автоматических обновлений и отслеживать подозрительные запросы, например, к неизвестным ZIP-архивам или пути /reports/MetricsUpload.