Проблема возникает из-за того, как настроена аутентификация в ALB. В частности, если клиенты неправильно настроят аутентификацию, злоумышленники могут использовать это для обхода контроля доступа и компрометации веб-приложений. Манипулируя передачей данных между ALB и сторонними службами аутентификации, злоумышленники могут получить несанкционированный доступ к конфиденциальным данным.

Исследователи Miggo обнаружили уязвимость во время работы с клиентом и нашли более 15 000 общедоступных приложений, которые могут быть уязвимы. AWS оспаривает это число, утверждая, что реальная цифра значительно ниже. После этого компания обновила свою документацию, включив в нее более безопасные методы реализации.