

Независимый исследователь безопасности под псевдонимом brutecat обнаружил уязвимость в системе восстановления доступа к аккаунтам Google. Ошибка позволяла определить личный номер телефона, привязанный к аккаунту, без ведома его владельца.

Суть проблемы заключалась в обходе системы защиты Google. Исследователь использовал цепочку действий, в том числе обход ограничений на количество попыток, чтобы перебором подобрать правильный номер телефона. По его словам, полностью автоматизированная атака могла занять менее 20 минут.

Чтобы подтвердить уязвимость, TechCrunch создали новый аккаунт с уникальным номером и дали его brutecat. Через короткое время он прислал правильный номер, подтвердив успешный взлом.

Опасность такой уязвимости в том, что зная личный номер, злоумышленники могли бы попытаться получить доступ к аккаунту через, например, подмену SIM-карты.

Google оперативно устранила баг и поблагодарила исследователя за помощь.