# Уязвимость StrandHogg 2.0 позволяет захватить контроль над любым Android-приложением


Исследователи безопасности компании Promon обнаружили в ОС Android новую опасную уязвимость повышения привилегий, позволяющую злоумышленникам получать доступ практическим ко всем приложениям на устройстве.

По классификации Google уязвимость, получившая идентификатор CVE-2020-0096 , является «критической». Исследователи из Promon назвали ее StrandHogg 2.0 из-за сходства с обнаруженной ими ранее уязвимостью StrandHogg.

Как и StrandHogg, StrandHogg 2.0 также позволяет злоумышленникам получать доступ ко всем приложениям на устройстве, но существенно расширяет поверхность атак. Кроме того, новый вариант сложнее обнаружить, что делает его «злым близнецом» предыдущей версии.

Эксплуатируя StrandHogg 2.0, злоумышленник может с помощью установленного на атакуемом устройстве вредоносного приложения похищать SMS-сообщения, фотографии и учетные данные, отслеживать местоположение по GPS, осуществлять звонки, записывать разговоры, а также шпионить за жертвой с помощью микрофона и камеры смартфона.

Google была уведомлена о проблеме в декабре 2019 года и в апреле 2020 года разослала своим партнерам исправление. Массовое развертывание патча запланировано на текущий месяц.

Источник: https://www.securitylab.ru/news/508671.php