УДК 004.056.5

Віталій Анатолійович Світличний,
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

Вразливість операційної системи Android

Американська компанія Nightwatch Cybersecurity (https://wwws.nightwatchcybersecurity.com), яка займається дослідженнями в області кібербезпеки, виявила критичну уразливість в операційній системі Android, причому у всіх її версіях старше 6.0. Як заявляють фахівці з компанії, знайдена в системі Android вразливість дозволяє отримати досить докладну інформацію про встановлених на мобільному пристрої додатках, конфіденційну інформацію про користувачів. Розкриття таких даних, як ім'я мережі Wi-Fi, BSSID, локальні IP-адреси, інформація про DNS-сервері і MAC-адресу пристрою відбувається без будь-якого дозволу з боку користувача і навіть без його відома. На перший погляд подібні дані здаються нешкідливими, проте з їх допомогою зловмисники можуть стежити за активністю користувачів в інтернеті і дізнаватися їх адреси проживання. Використовуючи ці дані, зловмисники за допомогою шкідливого програмного забезпечення можуть відстежити смартфон і навіть влаштувати атаку на бездротову мережу і інші підключені до неї пристрої. Завдяки уразливості Android хакерам також буде доступний весь вхідний і вихідний трафік на мобільному пристрої, логіни і паролі до облікових записів, а також особисті дані власника смартфона.

Вразливість пов'язана з внутрішньою функцією Android під назвою intents – «наміри», які використовуються для абстрактного опису операцій і дозволяють додаткам і операційній системі транслювати загальносистемні повідомлення, які можуть бути прочитані будь-якими додатками або компонентами. Ця функція дозволяє додаткам і самій операційній системі розсилати внутрішні повідомлення, доступні для читання всіма додатками і функціями на Android – пристрої. Як виявилося, мобільна операційна система від Google розкриває інформацію про Wi-Fi підключенні і Wi-Fi мережі через дві окремі функції intents – NETWORK_STATE_CHANGED_ACTION класу WifiManager і WIFI_P2P_

THIS_DEVICE_CHANGED_ACTION класу WifiP2pManager. Встановлені на пристрої додатки можуть прослуховувати ці intents і перехоплювати пов'язану з Wi-Fi інформацію, навіть якщо у них немає права на доступ до функції Wi-Fi. Фактично, дана вразливість дозволяє обійти систему дозволів Android. Зловмисники здатні обманом змусити користувача встановити невинне на перший погляд додаток, що збирає дані про Wi-Fi підключенні, а потім використовувати зібрані відомості для пошуку ідентифікаторів BSSID (таких як WiGLE або SkyHook) в доступних базах даних і виявлення домашньої адреси користувача.

Дана вразливість (CVE-2018-9489 докладніше тут: https://wwws.nightwatchcybersecurity.com/2018/08/29/sensitive-data-exposure-via-wifi-broadcasts-in-android-os-cve-2018-9489 /) зачіпає всі версії Android, в тому числі такі спеціалізовані операційні системи на зразок Amazon FireOS (для Kindle). Дослідники повідомили про неї компанії Google в березні поточного року, і компанія вирішила виправити вразливість, але тільки лише в версії Android 9.0 Pie. Згідно зі статистикою Google, вона встановлена поки на 0,1% всіх пристроїв на «Андроїд», а іншим користувачам, мабуть, доведеться змиритися – з більш старими версіями нічого робити не планується, так як, це буде серйозною зміною API. Звідси випливає практична рекомендація: для усунення даної уразливості користувачам слід виконати оновлення операційної системи до Android 9.0 Pie або більш пізньої 10 версії.

Одержано 25.10.2019