Cyberdefence 24

16.08.2018

FIRMOWE OPROGRAMOWANIE SMARTFONÓW MOŻE MIEĆ LUKI BEZPIECZEŃSTWA

Według ekspertów ds. cyberbezpieczeństwa z firmy Kryptowire, firmowe oprogramowanie dla niektórych smartfonów z Androidem zawiera luki bezpieczeństwa. Chodzi o takich producentów telefonów, jak LG, ZTE, Assus i Essential - donosi serwis The Verge.

Związani z Kryptowire badacze oceniają, że luki bezpieczeństwa w oprogramowaniu dostarczanym razem z telefonami powstają w procesie modyfikowania systemu operacyjnego Android przez producentów tych urządzeń.

Wykryte podatności mogą pozwolić atakującym m.in. na uniemożliwienie użytkownikowi telefonu dostępu do urządzenia (np. poprzez zmianę danych do logowania czy kodu odblokowującego), a także uzyskanie kontroli nad mikrofonem i galerią zdjęć oraz aparatem fotograficznym. W większości przypadków jednak - jak podkreślają eksperci - przeprowadzenie ataku wymaga od hakerów zainstalowania na telefonie złośliwego oprogramowania.

Badacze z Kryptowire oceniają, że przyczyną podatności bezpieczeństwa w firmowym oprogramowaniu na telefony z Androidem jest otwarty charakter tego systemu, który umożliwia producentom sprzętu na znaczące modyfikacje kodu. Firmy produkujące smartfony często dostosowują dzięki temu system operacyjny do swoich potrzeb, a nierzadko tworzą również całkowicie odmienne wersje Androida od tej, która jest dostarczana przez Google.

Według Kryptowire, luki w bezpieczeństwie spowodowane stosowaniem otwartego oprogramowania mogą też dotyczyć bezpieczeństwa sprzętowego smartfonów. Jak podkreślił szef firmy Angelos Stavrou, “wiele podmiotów uczestniczących w łańcuchu dostaw dla jednego producenta telefonów może chcieć tworzyć własne aplikacje i mieć wpływ na kod systemu, co tworzy dodatkowe powierzchnie ataku dla hakerów, a także zwiększa ryzyko występowania błędów w oprogramowaniu”.

Zdaniem ekspertów przykładem urządzenia, w którym występuje wiele tego rodzaju podatności i błędów bezpieczeństwa, jest smartfon Asus Zenfone V Live. Firma Kryptowire znalazła w nim luki pozwalające na całkowite przejęcie kontroli nad telefonem przez hakerów, a także na ingerencję atakujących w treść wysyłanych SMS-ów i możliwość przejmowania zdjęć, nagrań wideo, a także treści audio rejestrowanych przez mikrofon urządzenia.

W odpowiedzi na rezultaty audytu Kryptowire Asus oświadczył, że dysponuje wiedzą o podatnościach bezpieczeństwa swoich smartfonów i “pracuje nad ich szybką neutralizacją z pomocą odpowiednich łatek zabezpieczających dla oprogramowania”.

Badania Kryptowire współfinansowane były przez amerykańskie ministerstwo bezpieczeństwa wewnętrznego - informuje The Verge.