**Facebook, WeChat i inne popularne aplikacje ze znanymi podatnościami!**

**Zespół Check Point Research badając popularne programy mobilne odkrył, że wiele aplikacji ze sklepu Google Play, w tym Facebook oraz WeChat, są podatne na znane od dawna rodzaje ataków. W przypadku wykorzystania luk, zagrożone byłyby setki milionów użytkowników!**

Powszechnie sądzi się, że gdy tylko podatność zostanie odkryta, jest natychmiastowo łatana, przez co regularne aktualizowanie systemu operacyjnego i aplikacji pozwala na zachowanie bezpieczeństwa swojego urządzenia mobilnego.

**Jednak Check Point Research pokazuje, że nawet dawno załatane podatności mogą być krytycznie ważne, ze względu na to, że nieaktualny kod może znaleźć się nawet w najbardziej popularnych aplikacjach.**

Popularna aplikacja mobilna składa się zwykle z wielu „reużywalnych” komponentów napisanych w niskopoziomowym języku takim jak C. Komponenty te, zwane natywnymi bibliotekami, są często oparte na open sourcowych projektach lub zawierają fragmenty kodu z tego typu projektów.

*Gdy podatność zostaje znaleziona w projekcie, jest ona łatana, ale jego autorzy zwykle nie mają kontroli nad natywnymi bibliotekami, których może ona również dotyczyć, ani nad aplikacjami, które korzystają z tych bibliotek –* piszą na swoim blogu analitycy Check Point Research.**W ten sposób aplikacja może posiadać niezałataną wersję kodu nawet przez wiele lat po wykryciu podatności**. **I właśnie tego typu** trzy krytyczne luki w zabezpieczeniach zostały odnalezione w setkach popularnych aplikacji na Androida, w tym **Yahoo Browser, Facebook** czy **WeChat. Podatności te mogą umożliwić atakującemu kradzież danych aplikacji i zdobycie uprawnień systemowych, które posiada dana aplikacja, takich jak np. rozpoznanie lokalizacji użytkownika**

**Pełny materiał z analizą oraz filmem z pokazowego ataku dostępny jest pod linkiem:** [**https://research.checkpoint.com/2019/long-known-vulnerabilities-in-high-profile-android-applications/**](https://research.checkpoint.com/2019/long-known-vulnerabilities-in-high-profile-android-applications/)