**Smartfony Xiaomi były narażone na ataki Man-in-the-Middle!**

**Miliony użytkowników popularnych smartfonów Xiaomi zostało narażonych na ataki hakerskie – odkryli specjaliści bezpieczeństwa firmy Check Point Software Technologies. Poważna podatność znajdowała się w preinstalowanej aplikacji Xiaomi Guard Provider, mającej w domyśle zapewnić bezpieczeństwo urządzenia.**

Wykryta przez Check Pointa luka znajdowała się w jednej z preinstalowanych aplikacji na smartfonach firmy Xiaomi, będącej obecnie trzecim największym producentem telefonów komórkowych na świecie. Jak na ironię, podatność dotyczyła aplikacji bezpieczeństwa „Guard Provider”, która powinna chronić telefon przed złośliwym oprogramowaniem.

W związku z niezabezpieczonym ruchem sieciowym z i do aplikacji Guard Provider oraz wykorzystaniem wielu zestawów SDK w tej samej aplikacji, potencjalny haker mógł połączyć się z tą samą siecią Wi-Fi co ofiara i przeprowadzić tzw. atak Man-in-the-Middle (MiTM). Ze względu na luki w komunikacji między wieloma SDK atakujący mógł wprowadzić dowolny wybrany przez siebie kod, umożliwiający kradzież haseł, wgranie ransomware lub innego złośliwego oprogramowania czy śledzenie użytkownika.

Smartfony zwykle są dostarczane z fabrycznie zainstalowanymi aplikacjami, z których niektóre są przydatne, a inne nigdy nie są używane. Co więcej, podobnie jak większość tego typu aplikacji, Guard Providera nie można usunąć. Check Point po wykryciu dziury bezpieczeństwa, zgłosił ją Xiaomi, które następnie wydało łatkę uaktualniającą zabezpieczenia aplikacji.

**Xiaomi to jedna z ulubionych marek Polaków, która dzięki relatywnie niskim cenom odnosi imponujące sukcesy sprzedażowe. Jak niedawno poinformował polski oddział Xiaomi, cała dostępna pula najnowszego modelu Mi 9 wyprzedała się w Polsce w ciągu zaledwie jednego dnia.**

Pełna analiza podatności dostępna jest pod linkiem: <https://research.checkpoint.com/vulnerability-in-xiaomi-pre-installed-security-app/>