**Nawet połowa użytkowników smartfonów zagrożona!**

**Eksperci Check Point Research po 4-miesięcznym badaniu, znaleźli krytyczne podatności we wtyczce TrustZone Qualcomma. Wtyczka wykorzystywana jest w prawie połowie telefonów komórkowych na świecie i odpowiada m.in. za poświadczenie płatności mobilnych. Do tej pory uważana była za najbezpieczniejszy komponent w naszych smartfonach.**

Technicy Check Point Research w celu zbadania bezpieczeństwa modułu, zbudowali specjalny fuzzer, za pomocą którego znaleziono krytyczne podatności w aplikacjach Qualcomm TrustZone. Luki w zabezpieczeniach jednego z komponentów Trusted Execution Environment (ang. środowiska zaufanego uruchamiania) mogły potencjalnie doprowadzić np. do wycieku zabezpieczonych danych, rootowania urządzeń, odblokowywania bootloaderów, wykonywania niewykrywalnego APT.

TrustZone to wtyczka bezpieczeństwa wbudowana przez ARM w procesor Corex-A. Pozwala ona na stworzenie izolowanej, zabezpieczonej wirtualnej przestrzeni, w której system operacyjny może uruchamiać aplikacje zapewniając prywatność oraz łączność z bogatym systemem. Wirtualny procesor jest często określany jako „bezpieczny świat”, w porównaniu do „niezabezpieczonego świata”, w którym znajduje się REE (Rich Execution Environment), czyli bogate środowisko wykonawcze, oferowane przez same systemy operacyjne. W 2018 r. rynkowi tych procesorów przewodził właśnie Qualcomm z 45% udziałem w przychodach.

Wśród Trusted Execution Environment dla urządzeń mobilnych, wyposażonych w oparty na hardware protokół dostępu ARM wyróżnić można:

l Qualcomm’s Secure Execution Environment (QSEE, ang. Bezpieczne środowisko uruchomieniowe firmy Qualcomm), wykorzystywany w Pixelach, LG, Xiaomi, Sony, HTC, OnePlus, Samsung i wielu innych urządzeniach;

l Kinibi firmy Trustronic, wykorzystywany na urządzeniach firmy Samsung na rynki europejskie i azjatyckie;

l Trusted Core firmy HiSilicon, używany na większości urządzeń Huawei.

Check Point poinformował producentów o znalezionych lukach, a część z nich już wprowadziło łatki dla swoich urządzeń. Samsung załatał trzy luki w zabezpieczeniach. LG załatało jedną. Qualcomm również odpowiedział na zgłoszenie i załatał dziurę 13 listopada.

W wyniku przeprowadzonej analizy, firma Check Point Research wezwała użytkowników telefonów komórkowych do zachowania czujności i sprawdzania dostawców kart kredytowych i debetowych pod kątem nietypowych działań. W międzyczasie współpracuje ze wspomnianymi dostawcami w celu poprawy systemów bezpieczeństwa.