**Certifi-gate - czy Twoje urządzenie jest zagrożone?**

**Specjaliści firmy Check Point Software Technologies ostrzegają przed podatnością Certifi-gate\*, nękającą nawet do 60% urządzeń mobilnych z systemem Android. Wśród najbardziej zagrożonych są użytkownicy sprzętu LG, Samsung i HTC. Na początku sierpnia, podczas konferencji Black Hat USA 2015 w Las Vegas, specjaliści firmy Check Point Software Security ogłosili odkrycie podatności „Certifi-gate” w systemie Android, która dotyczy urządzeń największych producentów. W tym samym czasie Check Point udostępnił użytkownikom Androida aplikację umożliwiającą sprawdzenie podatności swojego urządzenia na powyższe zagrożenie.**

Certifi-gate Scanner został pobrany już blisko 100 tys. razy ze sklepu Google Play. Firma Check Point otrzymała ponad 30 tys. anonimowych wyników skanowania od użytkowników końcowych, dzięki czemu była w stanie określić narażenie na zagrożenia dla poszczególnych urządzeń, producentów i dostawców narzędzi Mobile Remote Support Tools (mRST).

Z analiz wynika, że użytkownik jest narażony na trzy zasadnicze rodzaje zagrożeń:

**Urządzenie podatne na zagrożenie**

Urządzenie jest podatne na zagrożenie Certifi-gate, zainstalowano podatną wtyczkę mRST, a aplikacja innego producenta wykorzystuje wtyczkę w celu uzyskania dostępu wyższego poziomu do urządzenia i jego wrażliwych zasobów. (tj. ekranu lub klawiatury itd.)

**Zainstalowana podatna wtyczka**

Urządzenie jest podatne na zagrożenie Certifi-gate, a na urządzeniu zainstalowano podatną wtyczkę mRST. Dowolna złośliwa aplikacja może uzyskać pełną kontrolę nad urządzeniem wykorzystując zainstalowaną wtyczkę.

**Zidentyfikowane podatne urządzenie**

Urządzenie jest podatne na zagrożenie Certifi-gate. Złośliwa aplikacja musi zainstalować podatną wtyczkę przed uruchomieniem exploitu (złośliwego kodu).

Według dostarczonych statystyk, najbardziej podatnymi na zagrożenia są urządzenia firmy LG – głównie przez wtyczki mRST (ponad 70% przypadków), a także HTC oraz Samsunga. Na przeciwległym biegunie znalazł się sprzęt mobilny firmy Sony, których większość (blisko 99%) została uznana za bezpieczne.

Recordable Activator zagrożeniem

Otrzymane przez Check Pointa wyniki skanowania Certifi-gate wskazują, że aplikację stosującą exploit zainstalowano na wielu urządzeniach. Recordable Activator, aplikacja opracowana przez brytyjską firmę Invisibility Ltd, którą pobrano od 100 tys. do 500 tys. razy ze sklepu Google Play, w skuteczny sposób wykorzystywała podatność Certifi-gate, omijając model uprawnień Android, korzystając ze wtyczki TeamViewer, by uzyskać dostęp do zasobów systemowych i zapisu danych ekranowych urządzenia.

Zdaniem zespołu badawczego firmy Check Point, deweloper „Recordable Activator” nie wykazał się w kwestii zabezpieczenia współpracy z innymi składnikami, a komunikacja ze składnikiem „Recordable Activator” może zostać zafałszowana bez jakiegokolwiek uwierzytelniania, umożliwiając dowolnej złośliwej aplikacji zapisanie danych ekranowych urządzenia.

**Aplikacja „Recordable Activator” wykazuje następujące nieodłączne problemy dotyczące Certifi-gate:**

1. **Aplikacje bez uprawnień mogą wykorzystać podatność, by przejąć pełną kontrolę nad urządzeniem bez konieczności żądania uprawnień od systemu Android.**

2. **Nawet gdy TeamViewer załatał wersję oficjalną, inne strony mogą w szkodliwy sposób nadużywać starych wersji wtyczki, by podejmować szkodliwe działania.**

3. **Istnieje możliwość wykorzystywania urządzeń mobilnych nawet, jeśli podatna wtyczka nie została preinstalowana na urządzeniu.**

4. **Aplikacje mogące wykorzystywać takie podatności można obecnie znaleźć w sklepie Google Play.**

5. **Jedynym rozwiązaniem problemu dla producentów jest udostępnienie podatnym urządzeniom zaktualizowanego ROMu.**

Certifi-gate to podatność, która pozwala aplikacjom na uzyskanie nieautoryzowanych praw dostępu, używanych zwykle przez aplikacje do zdalnego wsparcia, które są albo preinstalowane albo osobiście instalowane na urządzeniu.

Atakujący mogą wykorzystać Certifi-gate do uzyskania nieograniczonego dostępu do urządzenia, umożliwiając w ten sposób między innymi kradzież danych personalnych, śledzenie lokalizacji urządzenia czy włączenie mikrofonów celem nagrywania rozmów.