**Google Play Store piti saatavilla paikkaamattomia Facebook- ja WeChat-sovelluksia**

*Check Pointin tietoturvatutkijat ovat havainneet, että Googlen sovelluskaupassa tarjolla olevia, erittäin suosittujakin sovelluksia on jätetty päivittämättä. Hakkerit olisivat voineet halutessaan muokata Facebook-päivityksiä ja lukea WeChat-viestejä.*

**ESPOO – 21. marraskuuta 2019 –** Yleensä ajatellaan, että kun pitää ohjelmistonsa ja sovelluksensa päivitettyinä uusimpiin versioihin, on turvassa hakkereilta. Valitettavasti tämä ei pidä paikkaansa. Check Point Researchin tutkijat ovat todistaneet, että kaikki paikat eivät ole olleet paikoillaan esimerkiksi Facebookin ja WeChatin versioissa, jotka olivat tarjolla Googlen sovelluskaupassa.

Tutkijat kävivät viime kesäkuussa läpi satoja sovelluksia Google App Storen tarjonnasta ja tarkistivat, onko kolme tunnettua haavoittuvuutta korjattu niissä. Tulokset olivat hälyttävät. Vaikka päivitykset oli julkaistu, ne eivät olleet mukana kaikissa sovelluksissa. Periaatteessa pahantekijät olisivat voineet varastaa ja muokata Facebook-päivityksiä ja lukea WeChat-viestejä.

Check Point etsi ja löysi sovelluksista kolmea kriittistä ACE-haavoittuvuutta (arbitrary code execution), jotka ovat vuosilta 2014, 2015 ja 2016. Näiden aukkojen kautta on mahdollista ottaa sovellus hallintaan. Tulokset herättivät tutkijat kysymään, miten monta muuta paikkaamatonta haavoittuvuutta tarjolla olevista sovelluksista vielä löytyy.

Check Point kysyy myös, miksei Google valvo, että sovelluskehittäjät päivittävät sovelluksensa. Google tarjoaa kehittäjille mahdollisuuden päivittämiseen, muttei tällä hetkellä vaadi sitä. Check Point on ilmoittanut löydöksistään sovelluskehittäjille ja Googlelle ja toivoo, että tieto paikkaamattomista haavoittuvuuksista kannustaisi Googlea muuttamaan käytäntöjään.

Yleisöä Check Point kehottaa asentamaan puhelimilleen virustorjuntasovelluksen.

Tarkemmat tiedot tutkimuksesta löytyvät Check Point Researchin blogista: <https://research.checkpoint.com/>

**Lisätiedot ja haastattelupyynnöt:**

Maija Rauha, viestintäkonsultti, OSG Viestintä, maija.rauha@osg.fi, p. 0400 630 065

**Seuraa Check Point Researchia:**

Blogi: <https://research.checkpoint.com/>

Twitter: <https://twitter.com/_cpresearch_>

**Check Point Research**

Check Point Research huolehtii siitä, että Check Pointin asiakkailla ja laajemmalla tietoturvayhteisöllä on käytettävissään paras mahdollinen tieto kyberturvallisuuden riskeistä. Tutkijaryhmä kerää ja analysoi ThreatCloud-verkkopalvelun tallentamat maailmanlaajuiset kyberhyökkäystiedot, jotta hakkerit pysyvät kurissa ja kaikki Check Pointin tuotteet pystytään päivittämään uusimmilla suojauksilla. Tutkijaryhmä koostuu yli 100 analyytikosta ja tutkijasta, jotka tekevät yhteistyötä muiden tietoturvayhtiöiden ja viranomaisten kanssa.

**Check Point Software Technologies Ltd.**

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com/)) on johtava yritysten ja valtionhallinnon kyberturvallisuusratkaisujen tarjoaja globaalisti. Sen ratkaisut suojaavat 5. sukupolven kyberhyökkäyksiltä alan johtavalla haittaohjelmien, kiristysohjelmien ja muiden hyökkäysten kiinnijäämisprosentilla. Check Pointin monitasoinen tietoturva-arkkitehtuuri, ”Infinity” Total Protection sisältää 5. sukupolven (Gen V) edistyneen uhkientorjunnan, joka suojaa yrityksen pilvi-, verkko- ja mobiililaitteissa sijaitsevan tiedon. Check Point tarjoaa myös alan kattavimman ja intuitiivisimman yhden kontrollipisteen ohjausjärjestelmän. Check Point huolehtii yli 100 000 ison ja pienen yrityksen ja yhteisön tietoturvasta.