**Check Point Research löysi haavoittuvuuden, joka jätti Android-puhelinten takaoven raolleen tekstiviestihuijauksille**

*Haavoittuvuus koskee muiden muassa Samsungin, Huawein, LG:n ja Sonyn puhelimia.*

**ESPOO 5. syyskuuta 2019 –** Tietoturvayhtiö Check Pointin tutkimustoiminnasta vastaava Check Point Research on julkistanut löytämänsä tietoturva-aukon, joka jättää Samsungin, Huawein, LG:n, Sonyn ja muiden Android-älypuhelinten käyttäjät alttiiksi kalasteluyrityksille. Samsung ja LG ovat julkistaneet ohjelmistopäivityksen, joka korjaa haavoittuvuuden.

Android-puhelimissa on käytössä matkapuhelinverkon yli tapahtuva laitehallinta, over-the-air (OTA) provisioning, jonka avulla verkko-operaattorit lähettävät asetuksia ja päivityksiä puhelimiin. Check Point Research havaitsi, että tähän käytetyn Open Mobile Alliance Client Provisioning (OMA CP) -standardin tunnistautumismenetelmät ovat rajalliset. Ulkopuolisen on mahdollista esiintyä verkko-operaattorina ja lähettää käyttäjille väärennettyjä tekstiviestejä. Jos vastaanottaja hyväksyy uudet asetukset, hyökkääjä voi esimerkiksi reitittää puhelimen internet-liikenteen oman palvelimensa kautta.

Osassa Samsungin puhelimista laitehallinnan käyttö ei Check Pointin havaintojen mukaan edellyttänyt lainkaan tunnistautumista. Huawein, LG:n ja Sonyn puhelimissa oli tunnistautuminen, mutta se oli helppo ohittaa, jos hakkeri oli hankkinut käyttöönsä puhelimen käyttäjän IMSI-tunnuksen (International Mobile Subscriber Identity). Tunnuksen hankkiminen on mahdollista useilla eri tavoilla. Hyökkääjä voi esimerkiksi kätkeä puhelinsovellukseen koodin, joka lukee sovelluksen puhelimelleen ladanneen käyttäjän IMSI-tunnuksen. IMSIn voi ohittaa myös lähettämällä käyttäjälle tekstiviestin operaattorin nimissä ja pyytämällä häntä hyväksymään PIN-koodilla suojatun OMA CP -viestin. Käyttäjän pitää antaa PIN-koodi ja hyväksyä viesti, jotta hakkeri saa laitehallintaoikeudet.

”Android-puhelinten yleisyys tekee haavoittuvuudesta kriittisen. Puhelimen käyttäjällä ei ole mitään keinoa varmistua siitä, että laitehallintaan liittyvä OMA CP -tekstiviesti tulee luotettavasta lähteestä. On täysin mahdollista, että hän klikkaa viestiin ”hyväksy” ja päästää näin hyökkääjän sisään puhelimelleen”, sanoi tietoturvatutkija **Slava Makkaveev** Check Pointilta.

Check Pointin tutkijat ilmoittivat löydöksistään puhelinvalmistajille maaliskuussa. Samsung sisällytti paikan toukokuun tietoturvapäivitykseensä (SVE-2019-14073), LG julkisti korjauksensa heinäkuussa (LVE-SMP-190006), ja Huawei suunnittelee ottavansa korjaukset mukaan seuraavaan Mate- ja P-puhelinmallistojen sukupolveen. Sony ei ole ottanut haavoittuvuutta huomioon vaan toteaa, että heidän puhelimensa noudattavat OMA CP -määrittelyjä.

Check Point SandBlast Mobile auttaa suojaamaan älypuhelimet välistävetohyökkäyksiltä, kalastelulta ja haitallisilta OMA CP -viesteiltä. Lisätietoja osoitteesta <https://www.checkpoint.com/products/mobile-security/>

Tarkempia tietoja tutkimuksesta Check Point Researchin blogista:

<https://research.checkpoint.com/advanced-sms-phishing-attacks-against-modern-android-based-smartphones/>

**Lisätiedot ja haastattelupyynnöt:**

Rami Rauanmaa, Head of Security Engineering, Finland and Baltics, Check Point Software Technologies, ramira@checkpoint.com

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 tietoturvahteisöllä 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.