Uusi QuadRooter-haavoittuvuus uhkaa yli 900 miljoonaa Android-laitetta

Tietoturvayhtiö Check Pointin löytämät neljä uutta Android-laitteiden haavoittuvuutta tarjoavat hyökkääjille mahdollisuuden laitteiden hallintaan ja pääsyn arkaluontoisiin tietoihin.

8. elokuuta 2016 – Tietoturvayhtiö Check Point® Software Technologies Ltd:n tutkijat julkistivat Def Con 24 -tapahtumassa Las Vegasissa neljä uutta haavoittuvuutta, jotka koskevat yli 900 miljoonaa Android-laitetta.

Def Con 24 -tapahtumassa pitämässään esityksessä Check Pointin johtava mobiiliturvallisuuden tutkija Adam Donenfeld paljasti neljä haavoittuvuutta, jotka koskevat Qualcommin piirisarjaa käyttäviä Android-laitteita. Qualcomm on maailman suurin LTE-piirisarjojen valmistaja, joka vastaa 65 prosentista Android-laitteiden LTE-modeemeista.

Check Point antoi haavoittuvuuksille yhteiseksi nimeksi QuadRooter. Hyväksikäytettynä haavoittuvuus voi tarjota hyökkääjälle tilaisuuden koko laitteen hallintaan ja rajoittamattoman pääsyn arkaluontoiseen dataan. Hyökkääjä voi myös tallentaa laitteen näppäilyt, seurata GPS-dataa tai nauhoittaa ääntä ja videota.

Haavoittuvuus löydettiin Qualcommin piirisarjan ajureista. Hyökkääjä voi käyttää tietoturva-aukkoa hyväksi haittaohjelmalla, joka ei tarvitse käyttäjältä erikseen lupaa eri toimintojen suorittamiseksi. 900 miljoonan vaarassa olevan laitteen joukossa ovat myös nämä laitteet:

- Samsung Galaxy S7 & S7 Edge
- Sony Xperia Z Ultra
- Google Nexus 5X, 6 & 6P
- HTC One M9 & HTC 10
- LG G4, G5 & V10
- Motorola Moto X
- OnePlus One, 2 & 3
- BlackBerry Priv
- Blackphone 1 & 2

Koska ohjelmistoajurit ovat valmiiksi asennettu laitteisiin, voi haavoittuvuuden korjata vain asentamalla laitevalmistajan päivityksen. Laitevalmistajat taas voivat tarjota korjaavan päivityksen vasta saatuaan Qualcommilta korjatun ajuripaketin.

Check Point on julkaissut QuadRooter scanner -sovelluksen, joka on saatavilla Google Play -kaupasta. Sen avulla käyttäjät voivat kokeilla, onko oma laite mahdollisesti varassa. Linkki sovellukseen löytyy myös Check Pointin blogista: http://blog.checkpoint.com/

Check Point suosittelee seuraavia toimenpiteitä Android-laitteiden turvaamiseksi:

- Lataa ja asenna uudet Android-päivitykset heti, kun ne ovat saatavilla.
- Ymmärrä laitteen roottaamisen riskit.
- Vältä lataamasta sovelluksia mistään muualta kuin Google Playsta.
- Lue laitteen lupapyynnöt ennen kuin asennat sovelluksen. Varo sovelluksia, jotka pyytävät poikkeuksellisen laajoja oikeuksia, vaativat paljon tallennustilaa tai käyttävät paljon akkua.
- Käytä vain turvallisia langattomia verkkoja ja matkustaessa vain niitä, jotka ovat turvallisen tahon tarjoamia.
- Harkitse mobiililaitteen turvallisuutta parantavan ohjelman käyttöä.

Check Pointin tutkijat toimittivat tiedot löytämästään haavoittuvuudesta Qualcommille huhtikuussa 2016. Sen jälkeen tutkijat käyttivät tavallista käytäntöä (CERT/CC) antaa Qualcommille 90 päivää aikaa korjata haavoittuvuudet ennen niiden julkistusta. Qualcomm arvioi jokaisen haavoittuvuuden suuren riskin aukoksi ja on julkaissut paikkauksen laitevalmistajille.

Lisätietoa haavoittuvuudesta ja Check Point QuadRooter scanner -sovelluksesta: http://blog.checkpoint.com/

Lisätiedot ja haastattelupyynnöt:
OSG Viestintä, Toni Perez, toni.perez@osg.fi, p. 0400 630 063

Seuraa Check Pointia:
Check Pointin blogi: http://blog.checkpoint.com/
Twitter: www.twitter.com/checkpointsw
Facebook: https://www.facebook.com/checkpointsoftware
YouTube: http://www.youtube.com/user/CPGlobal