Check Point löysi haavoittuvuuksia johtavan drone-valmistajan palvelualustasta – löytö mahdollisti puutteiden korjaamisen

*Jos vikoja olisi hyödynnetty, niiden avulla olisi päässyt käsiksi DJI:n dronejen käyttäjätileihin.*

**SAN CARLOS, California – 8. marraskuuta 2018** – Tietoturvayhtiö Check Point Software Technologies ja maailman johtava drone- ja ilmakuvaustekniikkatoimittaja DJI kertoivat tänään yksityiskohtia haavoittuvuudesta, joka olisi voinut vaikuttaa DJI:n infrastruktuuriin, jos sitä olisi käytetty.

Check Point julkisti tutkimussivustollaan DJI:n Bug Bounty -ohjelman mukaisen raportin, jossa se kuvasi, millä tavoin hyökkääjä olisi voinut päästä käsiksi käyttäjätileihin. Haavoittuvuus oli DJI Forumin tunnistautumisjärjestelmässä. DJI Forum on laitteiden käyttäjille tarkoitettu, DJI:n ylläpitämä keskustelusivusto. Murtoriski liittyi siihen, että DJI:n eri alustat käyttivät asiakkaan tunnistamiseen samaa tunnistetta.

Potentiaalisessa vaarassa olivat DJI:n kuluttaja-asiakkaat, jotka ovat synkronoineet pienoiskopteriensa lentoja koskevat tiedot, mukaan lukien valokuvat, videot ja lentoreitit, DJI:n pilvipalvelimelle, sekä DJI:n yritysasiakkaat, joka käyttävät DJI FlightHub -ohjelmistoa, joka sisältää reaaliaikaisen kamera-, ääni- ja karttanäkymän. Haavoittuvuus on paikattu eikä sen hyödyntämisestä ole todisteita.

”Kiitämme asiantuntemusta ja vastuullisuutta, jota Check Pointin tutkijat osoittivat paljastaessaan potentiaalisesti kriittisen haavoittuvuuden”, kommentoi DJI:n Yhdysvaltain maajohtaja **Mario Rebello**. ”Juuri tämän takia perustimme Bug Bounty -ohjelmamme. Kaikki teknologiayhtiöt ymmärtävät, että tietoturvan varmistaminen on päättymätön prosessi. Asiakkaidemme tietojen pitäminen turvassa on DJI:lle avainasia, ja sitoudumme jatkuvaan yhteistyöhön Check Pointin ja muiden vastuullisten tietoturvatutkijoiden kanssa”, hän jatkoi.

”Ottaen huomioon, miten suosittuja DJI:n dronet ovat, on tärkeää, että tämän tapaiset, mahdollisesti kriittiset haavoittuvuudet korjataan nopeasti ja tehokkaasti, ja DJI on toiminut juuri siten. Yritysten ja organisaatioiden tulee ymmärtää, että niiden arkaluontoisia tietoja voidaan käyttää kaikilta eri alustoilta, ja jos ne ovat alttiina hyökkäyksille yhdellä alustalla, globaali infrastruktuuri saattaa olla vaarassa”, sanoi Check Pointin Head of Products Vulnerability Research **Oded Vanunu**.

DJI:n asiantuntijat luokittelivat Check Pointin löydöksen luokkaan korkea riski/matala todennäköisyys, koska hyökkääjän on täytettävä tietyt edellytyksen ennen kuin haavoittuvuutta voi hyödyntää. DJI tähdentää, että sen asiakkaiden tulisi aina käyttää DJI GO- tai GO 4 -ohjausohjelman uusinta versiota.

Check Point ja DJI kehottavat kaikkia käyttäjiä pysymään valppaina aina, kun tietoa siirretään digitaalisesti. Kaikessa verkossa tapahtuvassa kanssakäymisessä on hyvä muistaa hyvän tietoturvan vaatimukset, ja foorumeilla ja verkkosivuilla sijaitsevien linkkien suhteen on hyvä noudattaa varovaisuutta.

Yksityiskohtaisempi selostus haavoittuvuudesta löytyy Check Pointin tutkimusblogista:

<https://research.checkpoint.com/dji-drone-vulnerability/>

Lisäksi tapausta analysoidaan Check Pointin verkkosivujen blogissa: <https://blog.checkpoint.com/>

--

**Lisätiedot ja haastattelupyynnöt:**

Tietoturva-asiantuntija Rami Rauanmaa, Check Point Software Technologies, ramira@checkpoint.com

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

**Seuraa Check Pointia:**
Twitter: <http://www.twitter.com/checkpointsw>Facebook: <https://www.facebook.com/checkpointsoftware>Blogi: [http://blog.checkpoint.com](http://blog.checkpoint.com/)YouTube: <http://www.youtube.com/user/CPGlobal>LinkedIn: <https://www.linkedin.com/company/check-point-software-technologies>

**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 kohdistettujen hyökkäysten kiinnijäämisprosentilla. Check Pointin monitasoinen tietoturva-arkkitehtuuri käsittää uuden 5. sukupolven (Gen V) edistyneen uhkientorjunnan, joka suojaa yrityksen kaikkia verkko-, pilvi- ja mobiilitoimintoja kaikilta tunnetuilta hyökkäyksiltä, ja sitä hallitaan alan kattavimman ja intuitiivisimman yhden kontrollipisteen ohjausjärjestelmän kautta. Check Point huolehtii yli 100 000 ison ja pienen yrityksen ja yhteisön tietoturvasta.