

Merkittäviä haavoittuvuuksia OkCupid-treffipalvelussa – Check Point Research auttoi välttämään deittikatastrofin

Ilmaisen online-treffipalvelu OkCupidin käyttäjien arkaluontoiset tiedot olivat vaarassa – Check Pointin tutkijat havaitsivat, että hakkeri olisi voinut saada käsiinsä käyttäjien täydelliset profiilitiedot, yksityisviestit, kuvat ja sähköpostiosoitteet.

SAN CARLOS, CA. – 29. heinäkuuta, 2020 – Tietoturva-yhtiö [Check Point® Software Technologiesin](https://www.checkpoint.com) tutkijat havaitsivat äskettäin tietoturvapuutteita OkCupid-deittipalvelun sivustolla ja mobiilisovelluksessa. Hyödyntämällä haavoittuvuuksia hakkeri olisi päässyt käsiksi käyttäjien yksityisiin tietoihin ja olisi voinut esimerkiksi lähettää viestejä käyttäjien tileiltä heidän tietämättään.

Vuonna 2004 toimintansa aloittanut OkCupid on yksi eniten käytetyistä ilmaisista online-treffipalveluista maailmanlaajuisesti. Sillä on yhteensä yli 50 miljoonaa rekisteröitynyttä käyttäjää 110 maassa. Vuonna 2019 sivuston kautta järjestettiin keskimäärin 50 000 treffiä joka viikko. Koronaviruspandemian aikana OkCupidin keskustelujen määrä on lisääntynyt 20 %. Nettideittipalveluiden käyttäjien henkilökohtaiset tiedot houkuttelevat myös verkkorikollisia, jotka voivat käyttää niitä kohdistettuihin hyökkäyksiin tai myydä tiedot edelleen muille hakkereille.

Check Pointin tutkijat osoittivat, että OkCupidin sovelluksen ja verkkosivuston haavoittuvuudet voivat antaa hakkereille pääsyn käyttäjän täydellisiin profiilitietoihin, yksityisviesteihin, osoitteisiin ja kaikkiin OkCupidin profiilintiksymysten vastauksiin, mukaan lukien seksuaalinen suuntautuminen. Hakkeri olisi myös voinut manipuloida kohdekäyttäjän profiilitietoja ja lähettää tililtä viestejä muille käyttäjille vilpillisiä tarkoituksiaan varten.

Näin hyökkäys olisi voinut tapahtua:

1. Hakkeri luo haitallisen linkin, joka sisältää hyökkäystä varten kehitetyn haittaohjelman.
2. Hakkeri lähettää linkin aiottuun kohteeseen tai julkaisee sen julkisella foorumilla käyttäjien klikattavaksi.
3. Kun uhri klikkaa linkkiä sen avatakseen, haittaohjelma suoritetaan, jolloin hakkeri pääsee kohteen tilille.

Check Pointin Head of Products Vulnerability Research **Oded Vanunu** kommentoi: ”Havaintomme OKCupidista herättävät vakavia kysymyksiä kaikkien treffisovellusten ja -sivustojen turvallisuudesta. Osoitimme, että hakkeri pääsee käyttämään ja manipuloimaan käyttäjien yksityisiä tietoja, viestejä ja valokuvia. Jokaisen treffisovelluksen kehittäjän ja käyttäjän tulisi nyt pohtia varastoimensa ja jakamiensa henkilökohtaisten tietojen ja kuvien tietoturvan tasoa. Onneksi OkCupid ryhtyi välittömästi tiedon saatuaan paikkaamaan näitä haavoittuvuuksia mobiilisovelluksessaan ja verkkosivustollaan.”

Check Pointin tutkijat toivat havaintonsa ilmi OkCupidille, joka tunnisti ja korjasi palvelimensa tietoturvapuutteet. OkCupidin mukaan sovelluksen käyttäjät voivat jatkaa sen käyttöä turvallisesti. Potentiaalinen haavoittuvuus ei vaikuttanut yhteenkään käyttäjään, ja OKCupid korjasi sen 48 tunnin sisällä.

Lisätietoja haavoittuvuuksista ja video siitä, kuinka niitä voidaan hyödyntää:

<https://research.checkpoint.com>

Lisätietoja:

Maajohtaja Sampo Vehkaoja, Check Point Software Technologies, sampov@checkpoint.com.

Haastattelupyynnöt: Viestintäkonsultti Päivi Savolainen, OSG Viestintä, paivi.savolainen@osg.fi, p. 050 441 6068.

Seuraa Check Point Researchia:

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

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

Podcast: <https://research.checkpoint.com/category/cpradio/>

Facebook: <https://www.facebook.com/checkpointresearch>

Julkaisijasta:**Check Point Research**

Check Point Research (research.checkpoint.com) huolehtii siitä, että Check Pointin asiakkailta ja laajemmalla tietoturvyhteisöllä 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 suojausilla. Tutkijaryhmä koostuu yli 100 analyttikosta ja tutkijasta, jotka tekevät yhteistyötä muiden tietoturvyhtiöiden ja viranomaisten kanssa.

Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (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.