**Check Pointin tutkijat löysivät haavoittuvuuksia, joiden avulla hakkerit olisivat voineet kaapata Fortniten pelaajien tilit, tiedot ja pelivaluutan**

*Kyberrikolliset olisivat voineet aloittaa oman battle royalen pelaajia vastaan.*

**SAN CARLOS, CA — 16. tammikuuta 2018** – Tietoturvayhtiö Check Point® Software Technologies julkisti tänään yksityiskohtia haavoittuvuuksista, jotka vaaransivat supersuositun taistelupelin pelaajien yksityisyyden ja rahat. Haavoittuvuudet on jo korjattu.

Fortnitella on [lähes 80 miljoonaa pelaajaa](https://www.businessinsider.com/how-many-people-play-fortnite-stats-2018-2018-9?r=US&IR=T) kautta maailman. Fortnitea pelataan kaikilla pelialustoilla, mukaan lukien Android, iOS, konsolit kuten PlayStation4 ja Xbox One sekä Microsoft Windowsia käyttävät tietokoneet. Fortniteä pelaavat myös monet peliammattilaiset, joiden pelaamista voi seurata suorana verkossa, ja se on e-urheilun ystävien suosiossa.

Jos haavoittuvuuksia olisi hyödynnetty, hyökkääjä olisi saanut rajoittamattoman pääsyn pelaajan tilille ja hänen tietoihinsa sekä pystynyt hankkimaan pelivaluuttaa pelaajan luottokorttitiedoilla. Pelaajan yksityisyys olisi vaarantunut myös siten, että hyökkääjä olisi voinut kuunnella hänen pelin tuoksinassa käymiään keskusteluja. Myös huoneen taustaäänet olisivat olleet kuunneltavissa.

Fortniten pelaajiin on aikaisemmin kohdistunut huijausyrityksiä, joissa heitä on houkuteltu kirjautumaan valesivustoille, joissa olisi muka voinut saada käyttöönsä Fortninten pelirahaa (V-buck). Nyt löydetty haavoittuvuus olisi kuitenkin toiminut ilman kirjautumista uudelle sivustolle.

Havaitut kolme virhettä liittyivät kirjautumiseen Single Sign-On (SSO) -järjestelmän kautta, esimerkiksi Facebook-, Google- tai Xbox-salasanojen avulla. Hakkeri olisi voinut napata käyttäjän käyttöoikeustietueen (token) ja ottaa Fortnite-tilin haltuunsa. Pelaajan olisi pitänyt ainoastaan klikata hakkerin laatimaa kalastelulinkkiä, joka olisi tullut aidosta Epic Gamesin osoitteesta.

Ohjelmointivirheet sijaitsivat Epic Gamesin verkkosivujen kahdella alasivulla, joiden kautta hakkerin olisi ollut mahdollista järjestää napattujen tietojen uudelleenohjaus itselleen.

”Fortnite on yksi suosituimmista verkkopeleistä, joita lapset ja nuoret pelaavat, ja ohjelmointivirheet mahdollistivat massiivisen yksityisyyden menetyksen. Tämä ja äskettäin havaitut ongelmat [kuvauskopteriyhtiö DJI](https://research.checkpoint.com/dji-drone-vulnerability/):n pilvipalvelussa osoittavat, miten haavoittuvaisia pilvipalvelut ovat. Hakkerihyökkäykset näihin kohteisiin ovat yleistyneet, koska kyberrikolliset tietävät, että palvelut sisältävät paljon tietoa yhtiöiden asiakkaista. Kaksitasoisen tunnistuksen käyttöönotto on hyvä tapa ehkäistä vastaavan haavoittuvuuden hyödyntäminen”, kertoo Check Pointin tuotehaavoittuvuustutkimustyötä johtava **Oded Vanunu**.

Check Point ilmoitti löydöksistään Epic Gamesille, ja haavoittuvuus on nyt korjattu. Check Point ja Epic Games kehottavat pelaajia tarkkaavaisuuteen aina, kun tietoa siirtyy digitaalisesti, ja noudattamaan pelatessaan hyviä kybertapoja. Käyttäjäfoorumeilla ja verkkosivuilla sijaitseviin linkkeihin kannattaa suhtautua terveen epäluuloisesti. Kaksitasoinen tunnistautuminen on hyvä ottaa käyttöön aina kun mahdollista.

Vanhempien tulisi kertoa lapsilleen, että verkossa liikkuu myös rikollisia, jotka ovat kiinnostuneita heidän pelitileistään ja niiden sisältämistä tiedoista, ja että nämä henkilöt voivat yrittää huijata.

Organisaatioiden puolestaan tulisi tarkistaa IT-infrastruktuurinsa säännöllisesi vanhentuneiden verkkosivujen ja käytöstä poistuneiden, mutta löydettävissä olevien verkkotunnusten varalta.

Perusteellisemmat tiedot haavoittuvuuksista löytyvät Check Pointin tutkimusblogista: <https://research.checkpoint.com/hacking-fortnite/>

**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.