Tietoturva-aukko Amazon Alexa -virtuaaliavustajassa – mahdollisti salakuuntelun, tietovarkaudet ja IoT-laitteiden haltuunoton

Check Pointin tutkijat havaitsivat, että hakkerit saattoivat poistaa tai asentaa uhrin Amazon Alexa-tilin ”taitoja” sekä päästä käsiksi äänihistoriaan ja henkilökohtaisiin tietoihin.

SAN CARLOS, CA. – 13. elokuuta 2020 – Maailman johtavan tietoturvayhtiön Check Point Software Technologiesin tutkimustoiminnasta vastaava Check Point Research havaitsi äskettäin tietyissä Amazon/Alexa-aliverkkotunnuksissa tietoturva-aukkoja. Niiden kautta hakkerit olisivat voineet poistaa tai asentaa ”taitoja” (skills) uhrin Alexa-tilille sekä päästä käsiksi äänihistoriaan ja henkilökohtaisiin tietoihin. Tämä olisi vaatinut käyttäjältä yhden haitallisen linkin klikkauksen ja ääniaktivoinnin.

Alexa-virtuaaliavustajia on myyty maailmanlaajuisesti yli 200 miljoonaa. Se kykenee äänivuorovaikutukseen, hälytysten asettamiseen, musiikin toistoon ja älylaitteiden hallintaan kodin ohjausjärjestelmässä. Käyttäjät voivat kehittää Alexan kykyjä asentamalla siihen "taitoja" (skills), jotka ovat ääniohjattuja sovelluksia. Alexa-tileihin tallennetut henkilökohtaiset tiedot ja laitteen käyttö kodin automaatiojärjestelmän ohjaimena tekevät Alexasta houkuttelevan kohteen hakkereille.

Check Pointin tutkijat osoittivat, kuinka hakkerit saattoivat hyödyntää tiettyjä Amazon/Alexa-alidomainien haavoittuvuuksia lähettämällä uhrille haitallisen linkin, joka näyttää tulevan Amazonilta. Jos käyttäjä klikkaa linkkiä, hyökkääjä voi:

- Käyttää uhrin henkilökohtaisia tietoja, kuten pankkitietohistoriaa, käyttäjätunnuksia, puhelinnumeroita ja kotiosoitetta
- Päästä käsiksi uhrin puhehistoriaan Alexan kanssa
- Asentaa taitoja (skills-sovellukset) Alexa-tilille käyttäjän tietämättä
- Tarkastella käyttäjän Alexa-tilin koko taitoluetteloa
- Poistaa asennettuja taitoja käyttäjän tietämättä.

”Älykaiuttimet ja virtuaaliavustajat ovat niin arkipäiväisiä, että on helppo jättää huomiotta niiden rooli kodin älylaitteiden hallinnassa sekä se, kuinka paljon henkilökohtaista tietoa ne sisältävät. Mutta hakkerit näkevät ne pääsynä ihmisten elämään ja mahdollisuutena saada tietoja, salakuunnella keskusteluja tai tehdä muuta haittaa omistajan tietämättä", kertoo **Oded Vanunu**, Check Pointin Head of Products Vulnerabilities Research.

”Teimme tämän tutkimuksen tuodaksemme esiin, kuinka kriittistä näiden laitteiden turvaaminen on käyttäjien yksityisyyden säilyttämiseksi. Onneksi Amazon reagoi ilmoitukseemme nopeasti ja korjasi haavoittuvuudet. Toivomme, että vastaavien laitteiden valmistajat seuraavat Amazonin esimerkkiä ja tarkistavat tuotteensa haavoittuvuuksien varalta, jottei käyttäjien yksityisyys vaarannu. Aiemmin olemme tutkineet TikTokia, WhatsAppia ja Fortniteä. Alexa on huolettanut meitä jo jonkin aikaa, kun otetaan huomioon sen yleisyys ja yhteys IoT-laitteisiin. Juuri nämä mega-digitaaliset alustat voivat aiheuttaa eniten vahinkoa. Siksi niiden tietoturvatasolla on ratkaiseva merkitys”, Vanunu jatkaa.

Amazon korjasi ongelman pian sen jälkeen, kun siitä ilmoitettiin.

Näin suojaudut:

1. Älä asenna tuntemattomia sovelluksia älykaiuttimeesi.
2. Harkitse tarkkaan, mitä henkilökohtaisia tietoja jaat älykaiuttimesi kanssa (esimerkiksi salasanat, pankkitilit).
3. Hanki lisätietoja. Nykyään kuka tahansa voi luoda älyavustajasovelluksia, joten lue siitä lisää ennen asennusta ja tarkista sen tarvitsemat käyttöoikeudet.

Lue lisää Check Point Reseachin sivustolla ja katso videolta, kuinka haavoittuvuuksia olisi voitu hyödyntää.

Lisätiedot:
Rami Rauanmaa, Head of Security Engineering, Finland and Baltics, Check Point Software Technologies, ramira@checkpoint.com. Haastattelupyynnöt: Päivi Savolainen, viestintäkonsultti, OSG Viestintä, paivi.savolainen@osg.fi, p. 050 441 6068.

Seuraa Check Pointia:
Twitter: http://www.twitter.com/checkpointsw
Facebook: https://www.facebook.com/checkpointsoftware
Blog: http://blog.checkpoint.com
YouTube: http://www.youtube.com/user/CPGlobal
LinkedIn: https://www.linkedin.com/company/check-point-software-technologies

Check Point Research
Check Point Research (research.checkpoint.com) huolehtii siitä, että Check Pointin asiakkailla ja laajemmalla tietoturvayhteisöllä 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) 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.

