**Vakavin mahdollinen haavoittuvuus Microsoftin nimipalvelussa – vaatii toimia lähes kaikissa yrityksissä ja organisaatioissa**

*Check Point Researchin tutkijat havaitsivat toukokuussa Microsoftin Windows DNS -palvelimilla haavoittuvuuden, jolle Microsoft on antanut korkeimman mahdollisen riskiluokituksen. Microsoft on julkaissut tänään tiistaina päivityksen, joka paikkaa palvelinten tietoturva-aukon. Päivitys vaatii toimia useimmissa yrityksissä ja organisaatioissa.*

* Microsoft on tunnustanut haavoittuvuuden olemassaolon ja antanut sille korkeimman mahdollisen luokituksen, CVSS 10.0.
* Haavoittuvuus on ketjutuskelpoinen eli yksi onnistunut murto voi johtaa haavoittuvuuden sisältävien laitteiden automaattiseen ketjureaktioon kautta yrityksen.
* Check Point kehottaa yrityksiä ja organisaatioita paikkaamaan haavoittuvuuden. Paikka on mukana Microsoftin tämän viikon tiistaipäivityksessä.

**ESPOO — 14.7.2020** – Tietoturvayhtiö Check Point Software Technologiesin tutkija **Sagi Tzaik** löysi toukokuussa Windows DNS -palvelimista haavoittuvuuden, jonka kautta on mahdollista päästä käsiksi yrityksen tai organisaation koko IT-järjestelmään. Tietoturvariski koskee kaikkia Windows-käyttöjärjestelmiä vuoden 2003 versiosta lähtien. Check Point on antanut haavoittuvuudelle nimen SigRed.

DNS-palvelu eli nimipalvelu (Domain Name System) on yksi internetin kulmakivistä, jota ilman verkkoa ei ole mahdollista käyttää. Se on ”internetin puhelinluettelo”, joka kääntää kirjaimin ilmaistut osoitteet (kuten [www.checkpoint.com](http://www.checkpoint.com)) IP-osoitteeksi, numerosarjaksi, jonka perusteella tietokoneet pystyvät toimimaan. Useimmat yritykset ja organisaatiot käyttävät Microsoftin nimipalvelua riippumatta siitä, millainen IT-ympäristö niillä muuten on.

Check Point ilmoitti löydöksestään Microsoftille 19. toukokuuta. Microsoft tunnusti haavoittuvuuden ja julkaisi sitä koskevan paikan (CVE-2020-1350) tiistaipäivityksensä yhteydessä 14.7.2020.

Check Point suosittelee, että Windows-käyttöjärjestelmää hyödyntävät yritykset ja organisaatiot päivittävät DNS-palvelimensa välittömästi estääkseen haavoittuvuuden hyväksikäytön. Check Pointilla ei tiedetä, onko haavoittuvuutta hyödynnetty. Sitä pidetään kuitenkin todennäköisenä, koska Check Pointin tutkija löysi helposti parikin tapaa hyödyntää haavoittuvuutta. Joku muu on mainiosti voinut löytää samat reitit. Bugi on 17 vuotta vanha.

”DNS-palvelimen murto on vakava asia, koska sitä kautta on mahdollista päästä käsiksi koko organisaation IT-ympäristöön. Näin vaarallisia haavoittuvuuksia tulee julki erittäin harvoin. Riski koskee kaikkia organisaatioita, niin isoja kuin pieniäkin, joissa käytetään Windows DNS -palvelimia”, kommentoi Check Pointin haavoittuvuuksia tutkivan tiimin vetäjä **Omri Herscovici**.

”Tapaus osoittaa myös, että löytämistä odottavia haavoittuvuuksia on edelleen olemassa. Annoimme haavoittuvuudelle nimen SigRed ja uskomme, että sen paikkaamisen tulisi nyt olla IT-väen työlistalla päällimmäisenä. Tämä ei ole mikä tahansa haavoittuvuus”, tähdentää Check Pointin Suomen maajohtaja **Sampo Vehkaoja**.

Check Point on ainoa tietoturvapalveluiden tarjoaja, jolla on valikoimassaan SigRedin hyväksikäytön estävä ratkaisu.

**Näin suojaudut**

* Ota Microsoftin tarjoama päivitys käyttöön
* Suojaa organisaatiosi IT-järjestelmä nykyaikaisella tietoturvaratkaisulla
* Käytä hyökkäyksen torjumiseksi tätä CMD-komentoa:

reg add "HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters" /v "TcpReceivePacketSize" /t REG\_DWORD /d 0xFF00 /f net stop DNS && net start DNS

Tarkemmat tiedot haavoittuvuudesta Check Point Researchin blogista: <https://research.checkpoint.com/> ja Check Pointin blogista: <https://blog.checkpoint.com/>

**Lisätiedot ja haastattelupyynnöt:**

Sampo Vehkaoja, maajohtaja, Check Point Finland, [sampov@checkpoint.com](mailto:sampov@checkpoint.com)

Maija Rauha, viestintäkonsultti, OSG Viestintä, [maija.rauha@osg.fi](mailto:maija.rauha@osg.fi), p. 0400 630 065.

**Seuraa Check Point Researchia:**

Blogi: [blog.checkpoint.com/](https://blog.checkpoint.com/)

Twitter: [twitter.com/\_cpresearch\_](https://twitter.com/_cpresearch_)

**Check Point Research**

Check Point Research ([research.checkpoint.com](https://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](http://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.