

Windows-koneille hyökätään nyt pikakuvakkeiden kautta

19.7.2010 11:55 — Perttu Pitkänen
perttu.pitkanen@sanoma.fi

Microsoftin Windows-käyttöjärjestelmästä on löytynyt tietoturva-aukko, jolle ei ole vielä olemasta korjausta. Haavoittuvuutta käyttävä haittaohjelma leviää jo muun muassa usb-muistien avulla.

Microsoftin Windows-käyttöjärjestelmästä on löytynyt haavoittuvuus, joka liittyy käyttöjärjestelmän tapaan käsitellä lnk-päätteisiä tiedostoja.

Lnk-tiedostot ovat pikakuvakkeita, joita klikkaamalla Windows-käyttöjärjestelmässä avataan ohjelmia tai tiedostoja.

Haavoittuvuus koskee kaikkia Microsoftin uudempia käyttöjärjestelmäversioita ja niiden Service Pack -päivityspaketteja versiosta Windows XP SP3 lähtien. Myös beta-versiot tulevista Windows 7 Service Pack 1 ja Windows Server 2008 R2 Service Pack 1 -päivityspaketeista ovat haavoittuvia.

Tietoturvayhtiö [F-Securen mukaan](#) aukko on myös Windows XP Service Pack 2 -versiossa, mutta Microsoft ei ole listannut sitä [tiedotteessaan](#), sillä [ohjelmistoyhtiö on lopettanut sen tukemisen](#). F-Secure neuvoo version käyttäjiä poistamaan sovellusten linkkeinä toimivat kuvakkeet pois käytöstä.

Tietoturva-aukolle ei ole vielä olemassa korjausta.

Korjaamatonta haavoittuvuutta hyödyntävä haittaohjelma leviää saastuneiden usb-massamuistien välityksellä. Autorun/Autoplay-toiminnon käytöstä poistaminen ei estä haittaohjelman leviämistä.

Haittaohjelman tartunnan voi välttää päivittämällä virustorjuntaohjelmiston ja tarkistamalla kaikki tietokoneeseen liitettävät ulkoiset muistit.

Tietoturvayksikkö [Cert-Fi:n mukaan](#) levinneellä haittaohjelmalla tähdätään erityisesti teollisuusautomaatiojärjestelmiä vastaan. Haittaohjelma pyrkii piiloutumaan niin kutsuttujen rootkit-toimintojen avulla.

Erikoista on, että haittaohjelman rootkit-tiedostot on digitaalisesti allekirjoitettu Realtek Semiconductor -puolijohdevalmistajan aidoilla varmenteilla, jotka ovat jotenkin päätyneet hyökkääjien haltuun.

Vaikka allekirjoitukseen käytetty varmenne on vanhentunut, sitä voi edelleen käyttää [F-Secure](#).

Seuraava tiedossa oleva Microsoftin korjauspäivitys on 10. elokuuta.

<http://www.digitoday.fi/tietoturva/2010/07/19/windows-koneille-hyokataan-nyt-pikakuvakkeiden-kautta/20109954/66>