

Windows-aukkoon jo tunkua

24.10.2008 14:26 — Tuomas Linnake
tuomas.linnake@digitoday.fi

Microsoftin eilen paikkaamaan vakavaan Windows-haavoittuvuuteen on julkaistu tuotteistettu hyväksikäyttömenetelmä, Cert-Fi varoittaa.

Cert-Fi korostaa, että [kyseinen haavoittuvuus tiedostojen ja kirjoittimien jakopalveluissa](#) (sivun ensimmäinen kriittinen haavoittuvuus) koskettaa suurta määrää käyttäjiä, ja että useista lähteistä saatujen tietojen mukaan haavoittuvuutta käytetään jo aktiivisesti hyökkäyksissä.

Saatavilla on tuotteistettu keino hyväksikäyttää aukkoa. Tilanne on siis kärjistynyt eilisillasta, jolloin Microsoft vielä sanoi [ettei se ole nähnyt sellaista esimerkkikoodia](#) joka tepsisi tähän rpc-haavoittuvuuteen. Firma tosin tiesi rajoitetuista ja kohdennetuista hyökkäyksistä.

Viestintäviraston alaisen Cert-Fi:n tietoon ei kuitenkaan ole tullut suomalaisia hyökkäyksiä.

Hyökkääjien kanavia yritetään tukkia

Haavoittuva palvelu on oletusarvoisesti päällä Windows-järjestelmissä, joskin työasemissa palvelu on suljettu palomuuriasetuksin XP SP2 -järjestelmässä ja sitä myöhemmissä versioissa.

Palvelinympäristöt kuitenkin käyttävät palvelua ja sallivat liikenteen siihen tyypillisesti omien verkkojensa kohdalla. Näin ollen yksittäinen haavoittuva tietokone voi levittää haittaohjelmaa, kun se kytketään tähän verkkoon.

Cert-Fi:n tiedossa on myös, että useat kotikäyttäjät käyttävät palvelua. Tällöin palomuri ei suojaa haavoittuvuudelta niiden verkkojen osalta, joihin liikenne on sallittu.

Verkkoliikenne tcp-portteihin 139 ja 445 kannattaa oletusarvoisesti suojata verkon rajalla. Tämän lisäksi tulee kuitenkin kaikki verkon koneet päivittää mahdollisimman pikaisesti, tai ottaa niissä käyttöön jokin muu Microsoftin [tietoturvatiedotteessa MS08-067](#) luetelluista suojakeinoista.

Cert-Fi kertoo seuraavansa kansainvälisten kumppaneidensa kanssa haavoittuvuutta käyttävien haittaohjelmien levitystä verkossa. Levityskanavat pyritään sulkemaan mahdollisimman nopeasti, ja haittaohjelmanäytteet saatetaan myös virustorjuntayhtiöiden tietoon.

<http://www.digitoday.fi/tietoturva/2008/10/24/windows-aukkoon-jo-tunkua/200827801/66>