

Hakkerit nostavat meteliä hälyttävästä haavoittuvuudesta

16.1.2008 14:44 — Tuomas Linnake
tuomas.linnake@digitoday.fi

Hakkeriryhmä Gnucitizen varoittaa erittäin laajamittaisesta tietoturvahasta, jonka keskiössä on upnp-protokolla yhdessä Flash-animaatiotiedostojen kanssa.

Eri verkkoprotokollien kokoelma, josta käytetään nimeä upnp (universal plug and play), on hyvin laajalti käytetty esimerkiksi tavallisissa reitittimissä, jotka nököttävät internetiä käyttävien pc:iden vieressä. Myös Flash on varsin laajasti käytössä osana nettikokemusta.

[Ryhmän verkossa julkaisemien tietojen mukaan](#)

haavoittuvuus on riippumaton tietokoneen käyttöjärjestelmästä ja internet-selaimesta. Krakkeri voisi syöttää uhrille vaarallisen Flash-tiedoston (swf) esimerkiksi verkkosivun kautta, minkä jälkeen reititin olisi käytännössä kaapattu.

Pahimpana uhkana Gnucitizen pitää mahdollisuutta muuttaa uhrin internet-yhteyden dns-palvelin toiseksi. Sen jälkeen pahaa aavistamaton käyttäjä voisi esimerkiksi suunnata verkko-osoitteeseen google.fi tietämättä tai huomaamatta, että luotetun hakupalvelun sijasta hän onkin hyökkääjän laatimalla kopiosivulla. Ja haittaohjelmia puskee samalla sisään koneeseen.

Kyse on teoriasta, käytännössä hyökkäyksiä ei ole tapahtunut. Gnucitizen perustelee asian julkaisua sillä, ettei se voinut mennä yhdenkään valmistajan pakeille korjausta penätäkseen, koska kyseessä ei ole normaali ohjelmointivirhe. Puhutaan useiden erilaisten suunnitteluongelmien vyyhdestä, joten sormeja ei voi osoittaa suoraan kehenkään.

- Tämä on asia, joka on ratkaistava nyt heti ja ainoa keino siihen on tuoda julkisuuteen kaikki, mitä meillä on tiedossamme, Gnucitizen toteaa verkossa ([ongelman tarkempi tekninen kuvaus](#)).

Suositus on ottaa upnp pois päältä, vaikka tämä voi aiheuttaa ongelmia eri palvelujen käytössä.

<http://www.digitoday.fi/tietoturva/2008/01/16/hakkerit-nostavat-metelia-halyttavasta->

[haavoittuvuudesta/20081450/66](#)