

QuickTime ja Firefox muodostavat aukon

13.9.2007 16:51 — *Tuomas Linnake*
tuomas.linnake@digitoday.fi

Applen QuickTime Player -ohjelmisto ja Mozillan Firefox-selain saavat samaan työasemaan asennettuna aikaan haavoittuvuuden, Cert-Fi varoittaa.

Haavoittuvuuden on raportoitu koskevan osittain myös työasemia, joissa on sekä Apple QuickTime Player että Internet Explorer.

Aukko mahdollistaa muun muassa javascript-komentojen suorittamisen Firefoxin chrome-kontekstissa käyttäjän käyttöoikeustasolla.

Haavoittuvuudesta on toistaiseksi tarjolla vain vähän tietoa. Sen julkaisijan mukaan haavoittuvuutta on mahdollista hyväksikäyttää myös työasemissa, joihin on asennettu vain Internet Explorer, mutta lievemmin seurauksin. Haavoittuvuus saattaa lisäksi koskea myös muita selaimia.

Rajoittaminen mahdollista

Hyökkääjän on mahdollista suorittaa haavoittuvassa järjestelmässä muun muassa haluamiaan javascript-komentoja ja mahdollisesti saada haavoittuva järjestelmä hallintaansa esimerkiksi houkuttelemalla käyttäjä seuraamaan muotoiltuun xml-tiedostoon viittaavaa linkkiä.

Jos selainlaajennus on asennettu, edellä mainitun xml-tiedoston päätteenä voi olla mikä tahansa QuickTimen selainlaajennuksella suoritettavaksi määritetty tiedostotyyppi, esimerkiksi avi, mp3 ja niin edelleen. Jos selainlaajennusta ei ole asennettu, haavoittuvuutta voi helposti käyttää vain houkuttelemalla käyttäjä seuraamaan tietyllä tavalla muotoiltuun qtl-tyyppiseen tiedostoon viittaavaa linkkiä.

Haavoittuvuuteen ei ole olemassa ohjelmistokorjausta, mutta noscript-lisäosan asentaminen Firefox-selaimen suojaaa ainakin osalta hyväksikäyttöyrityksistä.

Lisäksi kieltämällä activex-komponenttien ja lisäosien suorittaminen Internet Explorerin suojausasetuksista

suojaakin osittain haavoittuvuuden hyväksikäyttöä, Cert-Fi neuvoo.

<http://www.digitoday.fi/tietoturva/2007/09/13/quicktime-ja-firefox-muodostavat-aukon/200722507/66>