

## Firefoxista paikattiin seitsemän reikää, Operasta kaksi

18.4.2006 09:43 — Tuomas Karvonen

Cert-Fi varoittaa sekä Firefox- että Opera-selaimen uusista haavoittuvuuksista. Firefoxin aukkoja hyväksikäyttämällä hyökkääjän voi olla mahdollista suorittaa kohdetietojärjestelmässä omia komentojaan, laajentaa omia käyttöoikeuksiaan tai varastaa tiedostoja.

Osa Firefoxin seitsemästä haavoittuvuuksista toimii tietyin rajoituksin myös Thunderbird-sähköpostiohjelmassa ja SeaMonkey-internet-ohjelmistossa.

Firefoxin ensimmäinen haavoittuvuus liittyy sivukomponenttien muokkaamiseen dynaamisesti. Hyökkääjän voi olla mahdollista varastaa kohdetietojärjestelmästä tiedostoja. Tiedostojen nimet täytyy olla valmiiksi tiedossa, jotta haavoittuvuutta voidaan hyväksikäyttää.

Toinen haavoittuvuus liittyy Firefoxin tapaan käsitellä tyylitiedostoja, kun taas kolmas koskee Firefoxin tapaa käsitellä dhtml-elementtejä. Kummatkin aukot voivat mahdollistaa hyökkääjälle komentojen suorittamisen.

Loput neljä haavoittuvuutta liittyvät esimerkiksi selaimen tapaan käsitellä xbl-kontrolleja, erilaisia mediakutsuja sekä xul-sisältöikkunoiden ja historia-mekanismien välisiä toimintoja. Aukot sallivat mahdollisesti komentojen suorittamisen tai laajennetut käyttöoikeudet kohdekoneella.

Haavoittuvuudet ovat Firefox-selainohjelmiston versiossa 1.5.0.1 ja sitä aikaisemmissa versioissa, Thunderbird-sähköpostiohjelman versiossa 1.5.0.1 ja sitä aikaisemmissa versioissa sekä SeaMonkey-internet-ohjelmiston versiossa 1.0 ja sitä aikaisemmissa versioissa. Päivitykset (Firefox, Thunderbird, SeaMonkey) ovat saatavilla.

### Operalla Flash- ja ylivuoto-ongelmia

Opera-selainohjelmistosta on myöskin löydetty haavoittuvuuksia, joita hyväksikäyttämällä hyökkääjän voi olla mahdollista suorittaa kohdetietojärjestelmässä omia

---

komentojaan.

Ensimmäinen haavoittuvuus liittyy Operan mukana tulevaan FlashPlayer-ohjelmistoon, josta löytyi useita haavoittuvuuksia.

Toinen haavoittuvuus on tyylitiedostojen käsittelyssä tapahtuva kokonaisluvun ylivuoto.

Cert-Fi:n mukaan haavoittuvuuksille ovat alttiina Operan versio 8.53 ja sitä aikaisemmat versiot. Selain on mahdollista päivittää.

<http://www.digitoday.fi/tietoturva/2006/04/18/firefoxista-paikattiin-seitseman-reikaa-operasta-kaksi/20066703/66>