

## Firefoxin tietoturvaongelmat jatkuvat, päivitys tulossa

20.11.2007 14:14 — Matias Mäki [matias.maki@sanoma.fi](mailto:matias.maki@sanoma.fi)

Avoimen lähdekoodin Mozilla Firefox -selaimesta löydettiin noin kaksi viikkoa sitten pari jar-protokollaan liittyvää xss-haavoittuvuutta, joiden avulla hyökkääjä pääsee penkomaan käyttäjän kohdepalvelimella sijaitsevia tiedostoja. Korjaukset haavoihin tekevät vielä tuloaan.

Gnucitizenin tietoturvatutkija, joka käyttää nimimerkkiä [lööpi](#) marraskuun 7. päivä sivustojen välisen ohjelmointihaavoittuvuuden Firefoxin jar-protokollan käsittelystä

**Jar:-protokollaa käytetään** Javan .jar-päätteisten zip-luokkapakettien avaamiseen ja käsittelyyn.

Haavoittuvuutta voidaan hyödyntää lähettämällä johonkin tiedostonjakopalveluun jar- tai zip-päätteinen haittatiedosto, joka käyttäjä houkuttelee avaamaan jar: -alkuisella osoitteella. Haitallinen paketti voidaan pakata myös kuvatiedoston loppuun, jolloin haavoittuvuutta voidaan hyödyntää myös kuvan avaamisella.

**Haitallisen paketin avaus** tarjoaa hyökkääjälle mahdollisuuden penkoa esimerkiksi uhrin käyttämän verkkopalvelun käyttäjäkohtaisia tietoja Javan ja selainten tietoturvarajoitusten sisäpuolella. Tämä vaatii sitä, että haittatiedosto sijaitsee saman nimitunnuksen alueella kuin mitä uhrin käyttämä palvelu.

**Sopivia kohteita** haavoittuvuuden hyödyntämiseen ovat useat web-palvelut, kuten web-sähköpostit, tiedostonjakopalvelut sekä monet web 2.0 -yhteisöpalvelut.

Käytännössä ongelma johtuu siitä, ettei Firefox tarkista avattavan paketin mime-tyyppiä. Ranskalainen [Frsirt](#) ja [tietoturvyhtiö Secunia](#) tuokittelevat haavoittuvuuden keskitason uhaksi.

**Pdp:n julkaistua löydöksensä** Mozilla julkaisi tiedot aiemmat tiedot ongelmasta. Näistä tiedoista käy ilmi, että [asiasta on raportoitu](#) projektin Bugzillaan jo viime

---

helmikuussa, mutta haava ei yksinään ole vielä vaarallinen. Kaveriksi se kaipaa vielä [http- ja jar-protokollien uudelleenohjausongelmiin liittyvän haavoittuvuuden](#) josta raportoitiin vasta marraskuun 10. päivä.

Selaimen kehittäjät työskentelevät paikkausten luomiseksi. Korjaukset sisältävää Firefoxin 2.0.0.10-versiota ei olla vielä julkaistu.

<http://www.digitoday.fi/tietoturva/2007/11/20/firefoxin-tietoturvaongelmat-jatkuvat-paivitys-tulossa/200729385/66>