

## Mozilla kehittää Firefoxia sotkemalla

6.8.2007 11:05 — Matias Mäki [matias.maki@sanoma.fi](mailto:matias.maki@sanoma.fi)

Mozillan Window Snyder ja Mike Shaver julkistivat Black Hat -tietoturvatapahtumassa Firefoxin kehittämisessä hyödynnetyn javascript-moottoreiden bugien ja haavoittuvuuksien etsimiseen tarkoitetun sotkijan.

Mozillan Window Snyder ja Mike Shaver julkistivat Black Hat -konferenssissa [jsfunfuzz](#) -sotkijan (fuzzer). Sen avulla kehittäjät voivat syöttää selainten javascript-tulkeille satunnaisesti sotkettua ja vääristeltyä koodia. Näin pystytään korjaamaan monia bugeja.

Julkistettu ohjelma ei testaa selainten dom (document object model) -toimintoja, vaan pelkästään javascript-moottoria.

[Jesse Rudemanin](#) kehittämän jsfunfuzzin avulla Mozilla Firefoxista on jo löydetty 280 bugia. Näistä kaksi tusinaa oli muistirajoihin liittyviä bugeja. Näitä olisi todennäköisesti voitu hyödyntää haittakoodin suorittamisessa selaimessa.

Snyder kertoi "Building and breaking the browser" -esityksessään, että sotkijaa voidaan hyödyntää myös muiden selainten toiminnan parantamiseksi. Mozilla onkin lähettänyt työkalun Microsoftille ja Operalle jo toukokuussa, muttei ole kuullut kuin Operasta. Nyt säätiö julkisti työkalun kaikille.

Operan testausjohtaja [Claudio Santambrogion mukaan](#) Opera-selaimesta on löydetty Mozillan työkalulla neljä kaatumistapausta, joista yksi voi olla tietoturva-avoittuvuus.

<http://www.digitoday.fi/tietoturva/2007/08/06/mozilla-kehittaa-firefoxia-sotkemalla/200718721/66>