

## Safari-selaimesta löytyi helppo haavoittuvuus

24.7.2010 10:43 — Tuomas Linnake  
[tuomas.linnake@digitoday.fi](mailto:tuomas.linnake@digitoday.fi)

Tutkija löysi "todella yksinkertaisen" haavoittuvuuden Applen Safari-selaimesta ja julkaisi esimerkkikoodin internetissä.

Mac-käyttäjän osoitekirjan henkilökohtaiset tiedot ovat vaarassa, hälyttää tutkija **Jeremiah Grossman** WhiteHat Securitysta. Safari-selaimen versiot 4 ja 5 sisältävät haavoittuvuuden verkkolomakkeita automaattisesti täydentävässä AutoFill-toiminnossa.

Hyökkääjä voisi luoda verkkosivun, joka onkii käyttäjän tiedot huomaamatta Mac OS X -käyttöjärjestelmän osoitekirjasta JavaScript-koodin avulla. Näihin tietoihin sisältyvät esimerkiksi nimi, työpaikka, kaupunki ja sähköpostiosoite.

Hyväksikäyttö on mahdollista, vaikka käyttäjä ei olisi koskaan kirjoittanut tietoja yhdellekään verkkosivulle [Grossman korostaa blogissaan](#).

- Tämä haavoittuvuus on niin yksinkertainen, että oletin jonkun toisen kertoneen siitä jo julkisesti. Mutta lukuisat etsinnät ja kyselyt tuottivat vesiperän, Grossman kirjoittaa.

### Puhelinnumeroteivät vuoda

Jeremiah Grossman on tehnyt haavoittuvuuden todentavan esimerkkikoodin, jonka julkaisi verkossa hänen pitkäaikainen kollegansa **Robert Hansen**. Heidät muistetaan muun muassa niin sanotun [clickjackin-vaaran esille nostamisesta](#).

Grossmanin mukaan ei ole takeita, etteikö Safarin aukkoa olisi jo voitu hyväksikäyttää hyökkäyksissä. Myönteistä on, että jostain syystä osoitekirjan numerolliset tiedot, kuten puhelinnumerot, eivät voi vuotaa haavoittuvuuden kautta.

Tutkija päätti julkistaa tietonsa sen jälkeen, kun Apple näytti suhtautuvan välinpitämättömästi hänen 17. kesäkuuta lähettämäänsä tiedonantoon. Haavoittuvuudelta voi suojautua kytkemällä AutoFill-toiminnon pois päältä.

---

## Laajempiongelma

Hyökkäys ei toimi Applen iPadissa, iPhonessa tai iPodissa. Grossman kuitenkin epäilee, että aukko ei koskisi vain Safaria, vaan olisi laajempi WebKit-selainmoottoria koskeva ongelma. Hän veikkaa, että Google Chromen vanhemmat versiot saattavat kärsiä samasta haavoittuvuudesta.

Lisäksi samankaltainen haavoittuvuus on hänen mukaansa myös Microsoftin Internet Explorer -selaimen vanhoissa versioissa 6 ja 7, [The Register -lehti kertoo](#).

Tutkija Jeremiah Grossmanin on määrä paljastaa ensi viikolla myös Firefoxin ja Chromen haavoittuvuuksia, jotka vaarantavat salasana. Hän pitää esitelmän Las Vegasin Black Hat -hackeritapaamisessa.

<http://www.digitoday.fi/tietoturva/2010/07/24/safari-selaimesta-loytyi-helppo-haavoittuvuus/201010245/66>