

Firefox razvija rigoroznu HTTPS zaštitu



Razvojni inženjeri Firefoxa testiraju [novu zaštitnu funkciju](#) [1] koja treba omogućiti povezivanje sa određenim web stranicama samo onda kada je kriptografskim certifikatom moguće potvrditi da je konekcija sigurna.

[Beta](#) [2] verzija preglednika sadrži listu web stranica koje primjenjuju [HTTP Strict Transport Security](#) [3] mehanizam. Radi se o mehanizmu koji zahtijeva od preglednika korištenje sigurnih SSL protokola tijekom komunikacije. HSTS omogućuje dodatni sloj zaštite tako što zahtijeva enkriptirani kanal i autentikaciju servera jakom kriptografijom.

Zamišljeno je da nova funkcija Firefoxa riješi ovaj problem koristeći listu preglednika koji koriste HSTS, te da spriječi povezivanje preglednika u slučaju kada određeni server nema valjani certifikat. Kako bi brže popunili svoju listu, Firefox iskorištava već kreiranu listu koju koristi Chrome (https://src.chromium.org/viewvc/chrome/trunk/src/net/base/transport_security_state_static.json) te svakom hostu šalje „*force https*“ zahtijev. Samo onaj koji odgovori sa valjanim HSTS zaglavljem i odgovarajuće velikom "max age" vrijednošću biva uvršten u listu.

Kada korisnik prvi put posjećuje neku od tih web stranica, preglednik će znati da mora koristiti sigurnu vezu tako da u slučaju kada napadač pokuša spriječiti sigurno povezivanje sa serverom, preglednik se neće povezati preko nesigurnog protokola, štiteći tako sigurnost korisnika.

Google Chrome već nudi sličan oblik zaštite o kojem se više može pročitati [ovdje](#) [4].

Na portalu je već bilo govora o [sigurnosti web preglednika](#) [5]. Iz članka se vidi da Firefox ne stoji dobro po tom pitanju, pa je svako poboljšanje zaštite korisnika dobrodošlo.

uto, 2012-11-06 12:03 - Ivan Sokač **Vijesti:** [Sigurnost](#) [6]

Kategorije: [Preglednici](#) [7]

Vote: 0

No votes yet

Source URL: <https://sysportal.carnet.hr./node/1134>

Links

[1] <https://blog.mozilla.org/security/2012/11/01/preloading-hsts/>

[2] <https://www.mozilla.org/en-US/firefox/channel/#beta>

[3] http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security

[4] <http://dev.chromium.org/sts>

[5] <https://sysportal.carnet.hr./node/1114>

[6] <https://sysportal.carnet.hr./taxonomy/term/13>

[7] <https://sysportal.carnet.hr./taxonomy/term/27>

