Razbijena PKI infrastruktura

Tim inženjera i sigurnosnih stručnjaka je objavio otkriće i potvrdu u praksi velikog sigurnosnog problema u samoj jezgri PK infrastrukture. Uz pomoć 200 playstation računala uspješno su kreirali lažni CA (Certification Authority) certifikat kojim su usjpešno prevarili sve uobičajene web preglednike uključujući Firefox i Internet explorer.

Napad iskorištava sigurnosnu ranjivost MD5 algoritma, koja omogućava kreiranje različitih poruka s istim MD5 hash-om. Iako je ranjivost u teoriji poznata već više godina, ovo je prvi put da ju je dokazano moguće iskoristiti za realni napad.

Iako je, već danas, većina certifikata potpisana teoretski sigurnijim SHA-1 algoritmom, kao rezultat ovog eksperimenta očekuje se prelazak svih preostalih CA servisa na korištenje SHA-1, te blokiranje lažnog proizvedenog CA u Firefoxu i Internet exploreru.

Kompletan izvještaj o napadu je objavljen na http://phreedom.org/research/rogue-ca/ [1], osim dijela koji pokriva sofisticirani algoritam za računanje MD5 kolizije, uz napomenu, da je to isključeno zbog zaštite internetske javnosti od ovog, zaista opasnog, tipa napada.

sri, 2008-12-31 11:48 - Ljubomir Hrboka**Vote:** 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/493

Links
[1] http://phreedom.org/research/rogue-ca/