IZPOVED »WHITE HAT« HEKERJA: KAKO SEM DOBIL TISTO DRAGOCENO DATOTEKO Z VAŠEGA RAČUNALNIKA

»WHITE HAT« HACKER'S CONFESSION: HOW I GOT THAT PRECIOUS FILE FROM YOUR COMPUTER

Luka Treiber

ACROS D.O.O.

Makedonska 113,

2000 Maribor

luka.treiber@acrossecurity.com

Povzetek

Ni naključje, da so spletni brskalniki za sodobne hekerje izjemno zanimivo in pogosto uporabljeno orodje vdiranja, saj so med najbolj razširjenimi aplikacijami na delovnih postajah. Predstavljajo most med »nevarnim« Internetom in varovanimi notranjimi omrežji. Njihova kompleksnost se je, odkar so se pojavili, dramatično povečala, zato je neizogibno, da se je povečala tudi količina varnostnih napak, ki jih vsakodnevno odkrijejo v njih. Pogosto je čas med odkritjem in varnostnim popravkom zelo dolg, tudi več mesecev, ali pa zaradi morebitnega zmanjšanja funkcionalnosti ranljivost sploh ni popolnoma odpravljena. Najbolj pereče so tiste varnostne napake, za katere zmotno velja, da ne predstavljajo resne grožnje. Varnostna napaka, ki omogoča lokalno izvajanje skript oziroma podtikanje skript v domeno lokalnega diska, je ena takšnih. V predstavitvi bomo pokazali, kakšne okoliščine privedejo do zlorabe tovrstne varnostne napake in kako resne so lahko posledice lokalnega izvajanja skript. Prikazali bomo tudi praktičen primer zlorabe omenjene varnostne napake v simuliranem okolju, kjer bomo navidezni žrtvi ukradli datoteke z gesli, osebne fotografije in na koncu njeno identiteto. Nazadnje bomo predstavili praktične ukrepe za obrambo pred tovrstnimi zlorabami in spletnimi napadi.

Abstract

Today web browsers are amongst the most utilized and the most attacked applications on workstation desktops. Since their beginning their complexity has increased dramatically, therefore the number of security vulnerabilities that are being discovered every day has also increased. Often the time between discovery and time of

Projekt delno financira Evropska unija iz Evropskega socialnega sklada ter Ministrstvo za šolstvo in šport.

vulnerability patch is very long and may take up to several months. Sometimes this is because of possible degradation of browser functionality that the vulnerability can not be fixed at all. The most problematical are those that are erroneously assigned a low severity. Local Cross-site Scripting is one of those. In our presentation we will point out the circumstances where we can fall prey to exploitation of such vulnerabilities and reveal the full potential of Local Cross-site Scripting. We will also demonstrate a Local Cross-site Scripting attack carried out in a simulated environment, stealing a virtual victim's password lists, personal photos and his identity. Finally, countermeasures will be provided on how to prevent such attacks.

Projekt delno financira Evropska unija iz Evropskega socialnega sklada ter Ministrstvo za šolstvo in šport.