Microsoftova praznična zakrpa

Pred samu novu godinu, 29.12.2011. Microsoft je izdao prekorednu zakrpu MS11-100, jubilarnu stotu i ujedno završnu za tu godinu. No iza te jednostavne vijesti krije se zanimljiva priča.

Dan ranije, 28.12., na konferenciji Chaos Communications Congress [1] u Berlinu, dvojica istraživača, Julian Wälde i Alexander Klink demonstrirali su kako izvesti DoS napad [2] na web site, šaljući posebno oblikovan upit koji preoptereti procesor na serveru za stotinjak sekundi. Radi se načinu obrade podataka u hash tablici, koji se može iskoristiti za napad uskraćivanjem usluge. Istog dana Microsoft je na Technetu objavio [3]analizu ranjivosti [4] [3]i ponudio privremeno rješenje za njezino izbjegavanje, dok još ne postoji zakrpa.

Već dan nakon njihova nastupa Microsoft je izdao zakrpu MS11-100, koja osim spomenute rješava još tri "privatno" prijavljene ranjivosti. Sve se odnose na ASP .Net. Brzina kojom je izdan ispravak mogla bi nas navesti na pomisao kako je Microsoft okrenuo ploču i kako će odsad istom brzinom ispravljati sve novootkrivene ranjivosti. U svjetlu nedavno objavljenog članka [5] u kojem se navodi da 55% otkrivenih ranjivosti ostaje bez ispravka nakon šest mjeseci, to bi zaista bio značajan i dobrodošao zaokret.

Ranjivost pogađa .Net od Windowsa XP, pa sve do servera 2008 R2 i Windowsa 7. Trebalo ju je isprobati na svim tim platformama, napraviti ispravke, testirati ih i sve to uredno dokumentirati. Nimalo lak posao, koji se ne može samo tako zbrzati i napraviti u jednom danu. Da ne spominjemo mugućnost da nakon izdavanja zakrpe neka od aplikacija koje su proizvod treće strane na serverima više neće ispravno raditi...

Iako su neki mediji čestitali Microsoftu na brzini, prava je istina je da je ranjivost, po nekim izvorima, poznata još od 2003 [6]. godine, dok je oCERT [7] obaviješten u rujnu 2011. i još je tada kontaktirao proizvođače softvera. Ranjivost ne pogađa samo .Net, već i druge web orijentirane programske alate, poput Perla, Rubyja i PHP-a, koji su već zakrpani, te Jave i Javaskripta, koji po svemu sudeći još nisu. Čekamo da se o tome izjasne Oracle i Google. Čini se da se ovdje ponavlja obrazac: javna objava ranjivosti ubrzala je izdavanje zakrpe čiji je razvoj već ranije započet. Na djelu je sukob Davida i Golijata: nekolicina istraživača koji se strastveno bave informacijskom sigurnošću bori se protiv tromih korporacija, kako bi zaštitili nas, obične smrtnike/korisnike.

Haker koji sebe naziva HybrisDisaster na Githubu je 7.1.2012 objavio dokaz [8] da je napad uspješan. Dovoljno je s jednog računala IIS-u poslati posebno oblikovanu datoteku i server će biti toliko opterećen da neće biti u stanju obrađivati druge zahtjeve. Ako još niste, odmah instalirajte zakrpu MS11-100.

pon, 2012-01-16 08:14 - Aco Dmitrović**Vijesti:** Sigurnost [9]
Kategorije: Servisi [10]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr./node/914

Links
[1] http://events.ccc.de/congress/2011/wiki/Welcome
[2] http://events.ccc.de/2011/12/28/crypto-talk-at-28c3-effective-denial-of-service-attacks-against-web-application-platforms-day-2-1400-saal-1/
[3] https://sysportal.carnet.hr./
[4] http://blogs.technet.com/b/srd/archive/2011/12/27/more-information-about-the-december-2011-asp-net-vulnerability.aspx
[5] https://sysportal.carnet.hr./node/913
[6] http://taz.newffr.com/TAZ/Reseaux/Techniques_Attaques/dos/CrosbyWallach_UsenixSec2003.pdf
[7] http://www.ocert.org/advisories/ocert-2011-003.html
[8] https://github.com/HybrisDisaster/aspHashDoS
[9] https://sysportal.carnet.hr./taxonomy/term/13
[10] https://sysportal.carnet.hr./taxonomy/term/28