Inicijativa "nultog dana"

Istraživači koji otkrivaju ranjivosti u softveru svoja otkrića ili prodaju na tržištu, uglavnom na Internetskim aukcijama, ili, ako se smatraju etičkim hakerima, upozoravaju proizvođače softvera očekujući da će ispraviti greške i zaštiti svoje kupce. Neki za svoje otkriće očekuju obeštećenje, kako bi naplatili utrošeno vrijeme. Međutim, mnogim se poznatim proizvođačima softvera ne žuri s izdavanjem zakrpa, što bi povremeno čak i etičke hakere nagnalo da ranjivosti i *exploite*, kod koji se može iskoristiti za napad, javno objave, nadajući se da će na taj način ubrzati izradu zakrpa.

HP-ova tvrtka Tipping Point, poznata po svojim Intrusion prevention uređajima, pokrenula je Zero Day Initiative [1], kako bi se regulirala objava ranjivosti. Istraživači sada mogu prijaviti otkrivenu ranjivost Tipping Pointu, koji procijeni njenu "vrijednost" prema šteti koju mogu izazvati. Otkupivši ranjivost, TP stiče "autorsko" pravo na nju i preuzima na sebe komunikaciju s proizvođačem softvera. Istovremeno, svojim zaštitnim uređajima dodaje filtere koji su u stanju prepoznati i zaustaviti napad, štiteći na taj način svoje klijente.

Proizvođačima softvera daje se rok od 180 dana za izdavanje zakrpe, a nakon toga se javno objavljuju ograničene informacije o ranjivosti, kako bi otežala izrada exploita, a istovremeno pojačao pritisak.

U 2011. godini TP je objavio 29 upozorenja o ranjivostima "nultog dana", nakon što proizvođači za šest meseci nisu izdali zakrpe. Deset su bile greške u IBM-ovom softveru, šest u HP-ovom i pet u Microsoftovom. Ostatak su podijelili CA, Cisco i EMC. Inače, ukupan broj ranjivosti koje je TP objavio u 2011. je 350, što predstavlja povećanje od 16% u odnosu na prethodnu godinu.

O sličnim problemima s ažurnošću ispravaka izvještava i IBM-ova ekipa X-Force. Po njima, oko 55% ranjivosti u 2010. nakon šest mjeseci ostalo je bez zakrpe, pa takvom nebrigom proizvođači softvera svoje kupce izlažu riziku. Neke ranjivosti čak ostaju nezakrpane godinama! Uskoro očekujemo izvještaj X-Forcea za 2011, pa ćemo vidjeti da li se nešto u međuvremenu promijenilo.

Redovita instalacija zakrpi nesumnjivo povećava sigurnost informacijskih sustava, no što učiniti u slučajevima kada zakrpe ne postoje? Za one koji si to mogu priuštiti, postoje zaštitni uređaji koji se prodaju pod nazivima *Intrusion Prevention System*, *Unified Threat Management*, ili *Next Genertion Firewall*, koji omogućuju takozvani "virtual patching", odnosno u stanju su prepoznati i zaustaviti napad koji je usmjeren na ranjivost koja nije zakrpana.

Naravno, pomaže i neprestan pritisak na proizvođače. Svako objavljivanje informacija o ranjivostima softvera predstavlja negativan publicitet, pa će se ulaganje u brzo ispravljanje grešaka dugoročno isplatiti jer razvija povjerenje kupaca u tvtku i njene proizvode.

čet, 2012-01-12 06:56 - Aco Dmitrović**Vijesti:** Sigurnost [2]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/913

Links
[1] http://www.zerodayinitiative.com/

[2] https://sysportal.carnet.hr/taxonomy/term/13