Ozbiljna ranjivost Internet Explorera

Microsoft je obznanio novotkrivenu ranjivost Internet Explorera, koja je dobila čudnovato ime: **use-after-free**. Ranjive su sve verzije IE od 6 do 11. Greška omogućuje napadaču izvršavanje koda na udaljenom računalu.

Ranjivost se iskorištava tako da se IE usmjeri na adresu objekta koji je prethodno izbrisan iz memorije, ili memorija nije na ispravan način alocirana. Time je objašnjeno ime ranjivosti: koristi memoriju nakon što je "oslobođena", odnosno ispražnjena. Greška izaziva korumpiranost memorije, što omogućava izvršavanje koda s privilegijama koje ima i sam korisnik. Napadači mogu kreirati web stranicu koja je oblikovana tako da iskorištava ovu ranjivost, te zatim namamiti žrtve da je posjete.

Microsof će izdati zakrpe nakon što bude završena analiza ranjivosti, a do tada se preporučuje nekoliko načina izbjegavanja:

- IE je na Windows serverima već postavljen u način rada koji se zove **Enhanced Security Configuration** [1] , čime je napad onemogućen.
- Podržane verzije Outlooka rade u načinu nazvanom **Restricted Sites zone**, pri čemu su isključene Active X kontrole. Provjerite da li su možda korisnici promijenili ovaj način rada u neki manje siguran. No ukoliko korisnik klikne na link u e-mailu, ranjivost se može iskoristiti za napad pomoću web stranice.
- Važno je da korisnici rade sa što manjim privilegijama, jer se time umanjuje moguća šteta, odnosno i napadački kod radi s manjim ovlastima.

Microsoft savjetuje da u postavkama Internet Explorera razina sigurnosti postavi na **High**, te da se koristi **Enhanced Mitigation Experience Toolkit 4.1**, (vidi Microsoft Knowledge Base Article 2458544 [2]).

Na kraju recimo i da je Microsoft propustio dati najjednostavniji savjet: dok ne izađe zakrpa, nemojte uopće koristiti Internet Explorer. Postoje i drugi preglednici, zar ne!

Link na Microsoftovu objavu:

https://technet.microsoft.com/en-US/library/security/2963983 [3]

uto, 2014-04-29 23:17 - Aco Dmitrović**Vijesti:** Sigurnost [4]
Kategorije: Preglednici [5]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1390

Links
[1] http://technet.microsoft.com/library/dd883248
[2] https://support.microsoft.com/kb/2458544
[3] https://technet.microsoft.com/en-US/library/security/2963983
[4] https://sysportal.carnet.hr/taxonomy/term/13
[5] https://sysportal.carnet.hr/taxonomy/term/27