Zakrpa za opasan Adobe Flash propust

Abobe je 20.02 objavio hitnu zakrpu [1] za Flash Player, nakon što je kompanija FireEye (https://www.fireeye.com/) ukazala na još jedan *zero-day exploit*. FireEye je tvrtka koja se bavi otkrivanjem, prevencijom i zaustavljanjem cyber napada. Malware koji su otkrili inficirao je web stranice tri neprofitne organizacije, od kojih se dvije fokusiraju na nacionalnu sigurnost i javnu politiku.

Predstavnici napadnutih stranica nisu odmah reagirali na komentare o napadima. Činjenica o kojim organizacijama se radi može dovesti do zaključka da napad ima za cilj prikupiti korisne podatke o vanjsko političkim zbivanjima i ekonomskim aktivnostima. Vjeruje se da napadači dolaze sa kineskog govornog područja, te da se možda radi o istoj grupaciji koja je odgovorna za cyber špijunažu [2] iz sredine 2012. godine.

Propust ugrožava Flash korisnike sustava Windows XP ili Windows 7, Javu 1.6 ili zastarjelu verziju Microsoft Officea 2007 ili 2010. Napad se obavlja ubacivanjem koda, a žrtve napada su preusmeravane na servere na kojima se nalazi *exploit* u skrivenom iframeu. Windows korisnici koji pokušavaju izbjeći napad trebali bi razmisliti o dogradnji sa XP na noviju verziju operativnog sustava, ažuriranje Jave i ažuriranje Officea. Iz FireEye-a napominju da čak ni dogradnja ne pruža kompletnu zaštitu, te vjeruju da napadači imaju dovoljno resursa da pronađu drugi način ugrožavanja korisnika. U svakom slučaju valja biti oprezan i pravovoremeno nadograđivati operacijske sustave i aplikacije.

Detaljnije možete pročitati slijedeć ovaj link [3].

pon, 2014-02-24 12:24 - Ivan Sokač**Vijesti:** Sigurnost [4]
Kategorije: Sigurnost [5]
Vote: 4

Vaša ocjena: Nema Average: 4 (1 vote)

Source URL: https://sysportal.carnet.hr./node/1358?page=0

Links
[1] http://helpx.adobe.com/security/products/flash-player/apsb14-07.html
[2] http://blog.shadowserver.org/2012/05/15/cyber-espionage-strategic-web-compromises-trusted-websites-serving-dangerous-results/
[3] http://www.pcworld.com/article/2099760/adobe-flash-exploit-targets-security-public-policy-sites.html
[4] https://sysportal.carnet.hr./taxonomy/term/13
[5] https://sysportal.carnet.hr./taxonomy/term/30