Ranjiv PowerPoint

Nakon što je prošlog utorka zakrpano osam ranjvosti, od toga tri ranjivosti [1] nultoga dana, Microsoft je objavio otkriće još jedne nove. Ovog je puta na meti je PowerPoint, a ranjivost je dobila oznaku CVE-2014-6352 [2].

Radi se o pogrešci u kodu koji obrađuje OLE objekte (*object linking and embedding*). Tu tehnologiju koriste sve uredske aplikacije, na primjer za ubacivanje Excell tablice u Word dokument, ili PowerPoint prezentaciju. Zasad su otkriveni mailovi kojima napadači šalju inficirane PowerPoint prezentacije, ali potencijalno su ranjive i ostale aplikacije iz MS Office paketa. Ova ranjivost napadaču daje ovlasti s kojima je pokrenut zlonamjerni kod.

Microsoft je izdao priopćenje [3] i privremenu zakrpu koja rješava Problem Powerpointa (*OLE packager Shim Workaround*), ali to nije potpuno rješenje i ostavlja ostale uredske aplikacije izložene napadu. Nadalje, zakrpa ne rješava ranjivost 64-bitnih verzija PowerPointa na Windowsima 8 i 8.1. Izlazak potpune, redovite zakrpe još se ne spominje.

Microsoft skreće pažnju korisnicima da ne zanemaruju upozorenja koje šalje *User Account Control* (UAC). U trenutku izvršenja zlonamjernog koda iskače prozor u kojem se traži dozvola za izvršavanje koda. Većina korisnika smatra takva upozorenja gnjavažom i rutinski daje dozvole, samo da mogu što prije nastaviti s poslom.

Među redovnim zakrpama izdanim ovog mjeseca ističe se rješenje za ranjivost CVE-2014-4114 [4], koja ugrožava Windows servere 2008 i 2012. Nju je koristio Sandworm, za kojeg se nagađa da je djelo ruske hakerske grupe. "Pješčani crv" (referenca na kultni SF roman Dune) korišten je za napade na računala Ukrajinske i Poljske vlade, NATO pakta i nekih zapadnih korporacija. Tu su i ranjivosti CVE-2014-4148 [5] koja omogućava da se iskoristi propust u obradi TrueType Fontova (TTF) i CVE-2014-4113 [6] koja omogućava dobijanje većih ovlasti na napadnutom računalu.

Ne preostaje nam drugo nego redovito instalirati sve nove zakrpe. Ali dok ne izađu prave zakrpe za OLE, postupajte oprezno s Office dokumentima koje dobijate od nepoznatih pošiljatelja, ali i od poznatih, ukoliko iz niste zatražili i ne očekujete ih.

čet, 2014-10-23 06:10 - Aco Dmitrović**Vote:** 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1444

Links
[1] http://thehackernews.com/2014/10/microsoft-patches-3-zero-day_15.html
[2] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6352
[3] http://support2.microsoft.com/kb/3010060
[4] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-4114

[5] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-4148
[6] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-4113