

Ranjivost nultog dana Microsoft Worda



Microsoft je jučer objavio svoj "security advisory" pod brojem 2953095 u kojem navodi kako je otkrivena ozbiljna ranjivost Worda. Ukoliko korisnik otvori datoteku u RTF formatu koja sadrži posebno priređene podatke, greška u parsiranju izaziva korumpiranost u sistemskoj memoriji što napadaču omogućuje udaljeno izvršavanje koda. Napadač dobija ovlasti koje na sustavu ima korisnik - još jedan primjer zašto je bolje raditi s ovlastima običnog korisnika, nego s administratorskim (eto prilike da to još jednom objasnite svojim "naprednim" korisnicima!). Napad je moguć i preko web stranica koje sadrže zlonamjernu RTF datoteku.

U priopćenju se navodi da je ranjiv Word od verzije 2003 do 2013, Microsoft Word Viewer (što ranjivim čini i Outlook), ali i Share Point 2010 - 2013, kao i Web Office apps 2010 - 2013. Microsoft je izdao privremeno, [brzo rješenje](#) [1] kojim se onemogućava otvaranje RTF dokumenata. Nakon detaljne analize ranjivosti bit će dostupna zakrpa koja trajno rješava problem.

Microsoft zahvaljuje Googleovom sigurnosnom timu jer su (krajem siječnja) objavili objavili svoje otkriće kao "Word RTF Memory Corruption Vulnerability ([CVE-2014-1761](#) [2])".

Ako želite saznati više, slijedite ove linkove:

<https://technet.microsoft.com/en-us/security/advisory/2953095> [3]

<http://thehackernews.com/2014/03/microsoft-word-zero-day-vulnerability.html> [4]

uto, 2014-03-25 20:49 - Aco Dmitrović **Vijesti:** [Sigurnosni propusti](#) [5]

Kategorije: [Software](#) [6]

Vote: 0

No votes yet

Source URL: <https://sysportal.carnet.hr/node/1371>

Links

[1] <https://support.microsoft.com/kb/2953095#FixItForMe>

[2] <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1761>

[3] <https://technet.microsoft.com/en-us/security/advisory/2953095>

[4] <http://thehackernews.com/2014/03/microsoft-word-zero-day-vulnerability.html>

[5] <https://sysportal.carnet.hr/taxonomy/term/14>

[6] <https://sysportal.carnet.hr/taxonomy/term/25>