Kritična ranjivost Media Playera

Istraživači tvrtke Trend Micro pronašli su posebno oblikovanu MIDI datoteku (*Musical Instrument Digital Interface*) koja će, ako je otvorite u Windows Media Playeru, na vaše računalo spustiti trojanca nazvanog TROJ_DLOAD.QYUA. Radi se o takozvanom *drive-by-download* napadu. Datoteka je objavljena na web stranici, pa će napast pokupiti surferi koji su se dali nagovoriti da poslušaju glazbu. Trojanac će dobiti ovlasti koje ima korisnik, što nas još jednom podsjeća koliko je opasno raditi s administratorskim ovlastima i naivno klikati po Mreži.

Ranjiv je Media Player svih inačica Windowsa osim W7 i Servera 2008 R2. Microsoft je zakrpu za ranjivost, koju je klasificirao kao kritičnu, izdao u siječanjskom paketu (MS12-004 [1]). Iz Microsofta kažu da se radi o dvije ranjivosti koje su im "privatno" prijavljene, što znači da su pomogli etički hakeri. Analiza napada dostupna je na blogu [2] istraživača Rolanda Dela Paza.

Ako je vaš Media Player podešen da se automatski ažurira, vjerojatno ste već dobili zakrpu. U protivnom, pobrinite se sami da je instalirate.

sub, 2012-01-28 07:17 - Aco Dmitrović**Vijesti:** Sigurnosni propusti [3]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/922

Links
[1] http://technet.microsoft.com/en-us/security/bulletin/ms12-004
[2] http://blog.trendmicro.com/malware-leveraging-midi-remote-code-execution-vulnerability-found/
[3] https://sysportal.carnet.hr/taxonomy/term/14