Procurio kod za iskorištavanje kritične ranjivosti RDP protokola

U paketu zakrpa za ožujak [1], Microsoft je izdao i zakrpu koja rješava ranjivost RDP protokola: *MS12-020 - Vulnerabilities in Remote Desktop Could Allow Remote Code Execution*. Požurite s instalacijom te zakrpe, jer se čini da je u opticaju *exploit* čije porijeklo izaziva kontroverze: naime čini se da ga je razvio sam Microsoft. Sada je u tijeku pranje ruku i prebacivanje odgovornoti za curenje koda.

Grešku i dokaz da se može iskoristiti, takozvani "proof of concept", prijavio je talijanski istraživač Luigi Auriemma još u svibnju 2011., i to HP/TippingPointovoj inicijativi nultog dana (Zero Day Initiative [2]). To je postao uobičajen način da se za otkriće dobije naknada, jer ZDI, za razliku od mnogih autora softvera, nagrađuje otkrivanje propusta u kodu. ZDI je sve uredno proslijedio Microsoftu. Čini se da je Microsoftov tim u studenom izradio program koji iskorištava ranjivost. Taj se kod pojavio na Internetu, u njemu su oznake koje ukazuju na Microsoft, poput teksta "MSRC11678". Sad se nagađa da li je kod procurio iz Microsofta, ili iz neke od antivirusnih tvrtki kojima je poslan kako bi olakšao izradu potpisa za prepoznavanje virusa. ZDI je izdao priopćenje u kojem energično poriče da su informacije procurile kod njih i upućuje sve da dodatne informacije potraže u Microsoftu. Uvidjevši da više nema razloga tajiti informacije, Auremma je i sam na svome siteu objavio prilog o otkriću. Ako već ne dobije nagradu, neka barem pobere slavu.

U međuvremenu, raspisana je nagrada od 1500 USD za izradu modula za Metasploit, popularni alat za penetracijsko testiranje.

Nama sistemcima ne preostaje drugo nego što prije instalirati zakrpe za ožujak.

Izvorni članak možete pročitati ovdje [3].

pon, 2012-03-19 12:16 - Aco Dmitrović**Vijesti:** Sigurnost [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/963

Links
[1] https://sysportal.carnet.hr/node/960
[2] https://sysportal.carnet.hr/node/913
[3] http://tinyurl.com/6wfu3k8
[4] https://sysportal.carnet.hr/taxonomy/term/13