Microsoft upozorava na ranjivost protokola MSCHAP v2


Microsoft je nakon nekoliko tjedana reagirao na izlaganje koje je na Defconu iznio istraživač Moxie Marlinspike, koji je demonstrirao kako probiti MSCHAP enkripciju.

MSCHAP v2 (Microsoft Challenge Handshake Authentication Protocol version 2) upotrebljava se pri autentikaciji korisnika koji se VPN-om spajaju izvana preko Microsoftova PPTP protokola (Point to Point Tunneling Protocol). Koristi se i pri bežičnoj WPA2 autentikaciji.

Iako se radi o dosta starom protokolu, koji se koristi još od vremena Widnowsa 98 i NT 4.0, još se uvijek masovno koristi, a podržavaju ga i Vista, Windows 7, Server 2003, 2008 i 2008 R2.

Marlinskpike je objavio program Chapchrack, koji iz mrežnog prometa izdvaja zaporke kriptirane MSCHAP protokolom, a zatim za njihovo dekodiranje koristi servis CloudCracker [1].

Nakon prisvajanja tuđeg identiteta napadač se može spajati u zaštićenu mrežu i koristiti sve ovlasti koje korisnik ima radi obavljanja posla.

Microsoft neće izdati zakrpu, jer se radi o slabosti alogoritma za enkripciju. Preporučuje se umjesto MSCHAP-a aktivirati PEAP (Protected Extensible Authentication Protocol). Upute za administratore dostupne su na ovom linku [2].

Prvi alati za probijanje MSCHAP protokola objavljeni su još prije pet godina (AsLEAP 2.1 [3]), tako se već dugo preporučuje napuštanje njegova korištenja.

Iako je Microsoft odaslao umirujuću poruku, tvrdeći da još nisu registrirani slučajevi napada koji koriste ovu ranjivost, preporučujemo da provjerite svoju konfiguraciju i aktivirate PEAP.

Radoznali mogu naučiti više na Marlinspikovom blogu. [4]

čet, 2012-08-23 09:45 - Aco Dmitrović**Vijesti:** Sigurnost [5]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1085

Links
[1] http://www.cloudcracker.com
[2] http://support.microsoft.com/kb/2744850
[3] http://www.willhackforsushi.com/?page_id=41
[4] https://www.cloudcracker.com/blog/2012/07/29/cracking-ms-chap-v2/

[5] https://sysportal.carnet.hr/taxonomy/term/13