Samba 3.5.0+ Remote Code Execution

I taman kako smo se zločesto nasmijali kolegama patnicima koji su zbog propusta u SMB protokolu i nezakrpanih Windows strojeva bili u panici za vrijeme trajanja nedavnog masovnog napada WannaCry ransomware zlotvora – eto nama sličnog propusta u Sambi.

Propust nije identičan, ali je slično neozbiljan: napadač može iskoristiti ranjivost u Sambi verzije 3.5.0 i novijih da na dijeljeni disk ubaci biblioteku zaraženu malicioznim kodom (ili samo maliciozni kod prerušen u biblioteku) i potom nagovori poslužitelj da taj maliciozni kod izvrši s administratorskim pravima.

Postoje tri načina ispravljanja ovog problema:

- instalacija sigurnosnih zakrpa za Sambu (4.6.4, 4.5.10, 4.4.14) koje jednom zauvijek rješavaju problem zloupotrebe named pipe funkcionalnosti;

- oni koji iz nekog razloga ne mogu instalirati zakrpe mogu problem zaobići tako što u /etc/fstab datoteci, u retku koji definira diskovni prostor iskorišten za Samba dijeljene direktorije, ubaci oznaku "noexec" – ovo je elegantno zaobilaženje problema, ali radi samo ako dijeljene direktorije ne držite na istoj particiji sa ostatkom Linux OS-a.

- ako ni to ne možete učiniti, možete dodati sljedeći redak u [global] sekciju smb.conf datoteke:

nt pipe support = no

međutim, budite oprezni jer ćete ovim isključiti named pipe funkcionalnost kroz IPC$, pa bi Windows klijenti mogli imati nuspojave: gubitak podrške za domenski kontroler na tom poslužitelju, nemogućnost stvaranja novih direktorija od strane Windows klijenata i slične sitnice koje život zagorčavaju.

Rješenje ovog potencijalno vrlo opasnog sigurnosnog problema nije strašno: sigurnosna nadogradnja, jednostavna izmjena u /etc/fstab kojom se zabranjuje izvršavanje koda sa particije na kojoj Samba drži dijeljene podatke (što bi, uostalom, trebala biti jedna od osnovnih sigurnosnih postavki takvog okruženja: odvojena particija za Sambu i na njoj "noexec", "nosuid" i "nodev" oznake), ili pak potpuno isključivanje IPC podrške za named pipes, što bi u nekim konfiguracijama moglo biti problematično – ali je jedino rješenje ako administrator ne može ili ne smije mijenjati verziju Sambe.

Također, valja nam podsjetiti kako je ovaj problem moguće ručno riješiti i na NAS uređajima za koje više ne postoji podrška i koji neće dobiti novu verziju Sambe: SSH protokolom valja se povezati na njih i aktivirati "noexec" oznaku na odgovarajućoj particiji (remountom ako nije moguće izmjeniti originalni fstab) – i sve će biti u redu.

Do otkrivanja nekog novog propusta kojeg neće biti tako jednostavno zaobići.

čet, 2017-05-25 10:30 - Radoslav Dejanović**Vijesti:** Sigurnosni propusti [1]
Kategorije: Servisi [2]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

story_tag: samba [3]

Source URL: https://sysportal.carnet.hr./node/1742

Links
[1] https://sysportal.carnet.hr./taxonomy/term/14
[2] https://sysportal.carnet.hr./taxonomy/term/28
[3] https://sysportal.carnet.hr./taxonomy/term/105