Re: Sårbarhet i social.telenor.com

From Telenor SOC <tsoc@tsoc.telenor.net>

To millie<millie@solem.dev>

Date Wednesday, July 3rd, 2024 at 1:09 PM

Hei,

Dessverre har vi ikke noe sånt for øyeblikket, men ser på mulighetene
for å lage noe sånt i fremtiden.

Du kan eventuelt bruke denne mailen som et takk for varslingen om svakheten.

Mvh
TSOC

On 02.07.2024 12:42, Millie Solem wrote:
> Hei,
>
> Nydelig, bra jobba! Ser ut som dere fjernet CNAMEen, så lenken funker ikke lenger. Forresten, har dere noen form for Security Hall-of-Fame eller lignende for å anerkjenne funn? Hvis så, hadde jeg satt pris på å ha navnet mitt på en slik liste, eller fått en attest på at jeg har bidratt til sikkerheten deres.
>
> Beste hilsen,
> Millie Solem
>
> On Wednesday, June 26th, 2024 at 3:22 PM, Telenor SOC <tsoc@tsoc.telenor.net> wrote:
>
>> Hei,
>>
>> Bekrefter at denne er mottatt og videresendt internt, så dette vil nok
>> ordnes. Takker for at du velger å varsle om dette!
>>
>> Med vennlig hilsen
>> Telenor Security Operations Center
>>
>>
>> On 25.06.2024 17:50, Millie Solem wrote:
>>
>>> Hei,
>>>
>>> Den følgende lenken dirigerer til en rickroll hostet på domenet mitt solem.dev
>>>
>>> http://social.telenor.com/w5aaa

>>>
>>> Dette er mulig som følge av en rekke sårbarheter. Jeg oppdaget dette for noen uker siden. Jeg varslet dette videre til en bekjent som jobber i Red Team hos dere; men i og med at sårbarheten ikke enda er patchet tenkte jeg det var på sin plass med et varsel på mail.
>>>
>>> Sårbarhetene utnyttet i den overnevnte lenken er som følger
>>>
>>> 1. dårlig DNS-konfigurering på social.telenor.com (direkte ekstern CNAME til PostBeyond)
>>> 2. mangel på kildevalidering hos leverandøren
>>> 3. siden lenken går gjennom vanlig HTTP uten SSL skjer heller ikke kildevalidering hos klienten (nettleseren)
>>> 4. mangelful entropi og "keyspace" i generering av URL-nøkler
>>> 5. felles pool av URL-nøkler for alle kunder hos leverandøren
>>>
>>> Disse sårbarhetene kombinert tillater for angrepet demonstrert over. En angriper kan lett se at domenet social.telenor.com bare er et CNAME til share.postbeyond.com, og at URL-nøklene kun er fem alfanumeriske tegn, som er ganske lett å bruteforce. Jeg gjorde det på en kveld. Deretter fant jeg en lenke til et utgått domene, kjøpte domenenavnet, og satt opp en redirect til nettsiden min.
>>>
>>> Patchen er enkel, men krever litt jobb. Beste løsning hadde vært å sette opp en egen self-hosted link shortener, og deretter migrere alle URL-nøklene deres fra PostBeyond over på den nye løsningen. Den nye løsningen kan deretter brukes til å opprette nye lenker med et bedre regime for generering av URL-nøkler (40 bits med entropi minimum, altså [A-Za-z0-9]{7}).
>>>
>>> Beste hilsen,
>>> Millie Solem
>>
>>
>> --
>> Telenor Security Operations Center
>> Support E-mail: tsoc-support@tsoc.telenor.net
>> Phone (24/7): +47 37018400
>> Mobile (24/7): +47 90712865
>

--
Telenor Security Operations Center
Support E-mail: tsoc-support@tsoc.telenor.net
Phone (24/7): +47 37018400
Mobile (24/7): +47 90712865