Zoomi videokonverentsi Windowsi rakenduses on paroole lekitav turvaauk

6 aastat tagasi - 01.04.2020 Autor: AM

Pandeemia ajal kodukontorites ülipopulaarseks saanud Zoomi videokonverentsiäpil on avastatud juba mitmeid turvaauke, mis tähelepanu keskmesse tõusnud tarkvaras häkkerite ja turvaekspertide poolt leitud. Viimane tänane suurem mure on Windowsi rakenduse juures nn. *UNC path injection* turvaprobleem, mille kaudu on võimalik Zoom´i Chat´is ehk vestluses ründajal näpata Windowsi parool, kui kasutaja klõpsab kahtlasel lingil.

Bleeping Computer kirjutab, et saadetud tekstilised lingid tehakse automaatselt klõpsatavateks, mis avanevad kasutaja arvuti veebilehitsejas ning samamoodi tehakse ka Windowsi UNC aadressidega (*Universal Naming Convention*). Pahaaimamatu kasutaja võib klõpsata näiteks lingil **\\evil.server.com\images\cat.jpg** ja loodab näha kassipilti, kuid tema andmed saadetakse samal ajal kuhugi serverisse.

Windows saadab vaikimisi UNC aadresside \\ puhul vastuvõtvasse serverisse Windowsi kasutajanime ning nõrgalt krüpteeritud salasõna, et seda pilti avada. Nn. NTLM hash küll parooli kohe ei paljasta, kuid spetsiaalsete tarkvarade (Hashcat või Dehash) ning piisava arvutusvõimsusega on võimalik salasõna hashist lahti murda mõne minutiga.

Zoomile on turvaaugust teada antud - tarkvaras tuleb teha muudatus, et UNC aadresse ei teisendataks automaatselt klõpsatavateks linkideks. Enne aga, kui võimalik uuendus saabub, soovitatakse oma arvutis vaikimisi seaded ära muuta:

Computer Configuration -> ***Windows Settings*** -> ***Security Settings*** -> ***Local Policies*** -> ***Security Options*** -> ***Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers*** ja valida *Deny all.*

Vaata lähemalt siit.

Ühtlasi tasub olla ettevaatlik ka Zoomi tarkvara allalaadimisega. Õige koht on https://www.zoom.us, kuid netis levib väga palju libalehekülgi. Check Point on kirjutanud, et kodukontorites ootamatult suure populaarsuse osaliseks saanud Zoomi nimele sarnaste domeenide registreerimine on kasvanud plahvatuslikult ja kõik need uued domeenid pole lihtsalt niisama süütud eksitamis-saidid. Lisaks

levib netis ka kahtlasi faile, mis pole tegelikult Zoomi videokonverentsi originaal-installerid. Check Pointi andmetel on libainstallerid näiteks nimega zoom-us-zoom_#########.exe” ja “microsoft-teams_V#mu#D_#########.exe”, kus # tähistab suvalisi numbreid. Ja see ei ole aprillinali.

- Uudised
- Turvalisus

Pilt