Tel. 1805
El. p. cert@nksc.lt
https://www.nksc.lt

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS
PRIE KRAŠTO APSAUGOS MINISTERIJOS

INFORMACINIS BIULETENIS DĖL INTEGRUOTOS VAIZDO, TELEFONIJOS IR POKALBIŲ PLATFORMOS „ZOOM“ SAUGUMO SITUACIJOS

2020 m. balandžio 22 d., atnaujinta gegužės 12 d.

Dėl nustatytų „Zoom“ programos saugumo spragų, rekomenduojame nenaudoti šios programos ypatingos svarbos informacinių infrastruktūrų bei viešojo sektoriaus informacinėse sistemose, skirtose tarnybinės informacijos apsikeitimui, iki to momento, kol nebus gamintojo išleisti saugumo atnaujinimai, kurie pašalins rizikas dėl informacijos saugumo ir asmens duomenų praradimų.

Pažymėtina, kad nematome problemos naudoti „Zoom“ versiją 5.0 (arba naujesnę) nuotoliniam mokymo procesui, viešos ir ne konfidencialios informacijos apsikeitimui, kai laikomasi žemiau aptartų saugumo rekomendacijų:

1. Vaizdo konferencijos metu rekomenduojama naudotis tik vaizdo funkcionalumu, o susirašinėjimams pasirinkti kitą komunikacijos priemonę arba naudoti „Zoom“ platformą per naršyklę, pačios sistemos į įrenginį neįdiegiant. Naudojant versiją naršyklėje reikia būti itin atidžiais, kadangi sparčiai plinta „Zoom“ svetainės klastotės, kuriose bandoma surinkti vartotojų duomenis arba priversti atsisiųsti kenkėjišką programinį kodą.

2. Organizacijos neturėtų „Zoom“ pokalbio kanalų identifikacinio numerio (ID) skelbti viešai, pokalbių kambariai turėtų būti apsaugoti slaptažodžiais. Minėta

Tel. 1805
El. p. cert@nksc.lt
https://www.nksc.lt

„Zoom“ versija 5.0 jau turi pokalbių kanalų apsaugą slaptažodžiu savo standartiniuose nustatymuose.

3. Vartotojus į pokalbio kambarį rekomenduojama įtraukti per virtualų laukiamąjį (*angl.* Waiting-room), o ekranu dalintis (*angl. Share-screen*) leisti tik pokalbio organizatoriui. Ekrano dalinimosi metu paisyti „švaraus darbastalio“ etiketo.

4. Kai naudojama „Zoom“ programa, rekomenduojama griežtai naudoti tik pačią naujausią versiją (š. m. gegužės 12 d. tai versija 5.0.2 (24046.0510)).

5. Įvertinti turimų įrenginių saugumo charakteristikas – vartotojams jungiantis iš pažeistų sistemų, konferencijos programos saugumas įtakos neturės. Būtina išlikti budriems ir kritiškai vertinti gaunamas nuorodas ir siunčiamas rinkmenas (failus).

6. Paisyti bendrųjų kibernetinio saugumo rekomendacijų, pateiktų NKSC prie KAM internetiniame puslapyje: *https://www.nksc.lt/rekomendacijos.html*

„ZOOM“ SITUACIJOS BENDRA APŽVALGA

Verslui ir institucijoms pradėjus vykdyti dalį veiklos nuotoliniu būdu, ženkliai išaugo nuotolinės komunikacijos poreikiai. Dėl savo patogumo ir paprasto naudojimo išpopuliarėjo vaizdo konferencijų ir pokalbių platforma „Zoom“. Tačiau ši sistema susilaukė daug dėmesio ir dėl savo neigiamų aspektų. NKSC įspėja apie platformos pažeidžiamumus, duomenų privatumo problemas ir didėjantį kiekį sistemos klastočių, per kurias bandoma išgauti konfidencialius vartotojų duomenis ir užvaldyti jų įrenginius. „Zoom“ ėmėsi veiksmų ir ištaisė keletą spragų bei duomenų privatumo pažeidimų, o taip pat pažadėjo artimiausiu metu visą dėmesį skirti būtent saugumo gerinimui, o ne naujų funkcionalumų diegimui. Vis tik komunikacijos platformos naudotojai turėtų išlikti atsargūs. Sistema neturėtų būti naudojama konfidencialiems duomenis persiųsti.

„Zoom Video Communications“ („Zoom“) yra kinų kilmės verslininko Eric Yuan 2011 m. JAV įkurta ryšių technologijų įmonė, kurioje dirba virš 2 500 darbuotojų [1]. „Zoom“ 2019 m. apyvarta – 620 mln. JAV dolerių, įmonė listinguojama JAV NASDAQ vertybinių popierių biržoje [2].

Įmonės žinomiausias produktas – integruota vaizdo, telefonijos ir pokalbių platforma „Zoom“, veikianti debesų kompiuterijos pagrindu. Remiantis įvairiais šaltiniais, „Zoom“ užima stiprias pozicijas šiuolaikinių vaizdo ryšių rinkoje [3]. Verta pažymėti, kad Toronto universiteto (Kanada) tarpdisciplininės laboratorijos „The Citizen

Tel. 1805
El. p. cert@nksc.lt
https://www.nksc.lt

Lab“ atliktame tyrime teigiama, kad „Zoom“ aplikacija yra kuriama trijų Kinijos įmonių, turinčių vienodus „Ruanshi Software“ pavadinimus. Vertinama, kad produkto vystymui Kinijoje „Zoom“ remiasi apie 700 darbuotojų turinčiais žmogiškaisiais tyrimų ir plėtros resursais [4].

Įvairių ekspertų vertinimu, platforma pasižymi paprastumu vartotojui, patikimu vaizdo ir garso pokalbių ryšiu [5]. Platforma galima naudotis ir neturint specializuotos programinės įrangos – „Zoom“ pasiekiama per interneto naršyklę.

Platesnį funkcionalumą užtikrina įmonės sukurti nemokami programinės įrangos paketai ir mob. aplikacijos, veikiantys įvairiuose įrenginiuose. Mobiliesiems telefonams ir planšetiniams kompiuteriams „Zoom“ prieinamos Google „Play“ ir Apple „App Store“ mob. programų parduotuvėse [6], o programinės įrangos paketus stacionariems ar nešiojamiems kompiuteriams (Windows, Linux ar macOS sistemoms) [7] galima atsisiųsti iš „Zoom“ internetinio puslapio [8].

Norint naudotis „Zoom“ platformos paslaugomis, vartotojai turi joje užsiregistruoti. Nemokamai vartotojai gali kurti iki 100 dalyvių turinčius pokalbių kambarius, veikiančius 40 min. sesijomis. Sesijos laikui pasibaigus, vartotojai nuo pokalbių kambario automatiškai atjungiami, ir sesija užbaigiama. Jeigu pokalbių kambaryje yra du vartotojai, sesijos trukmė neribojama.

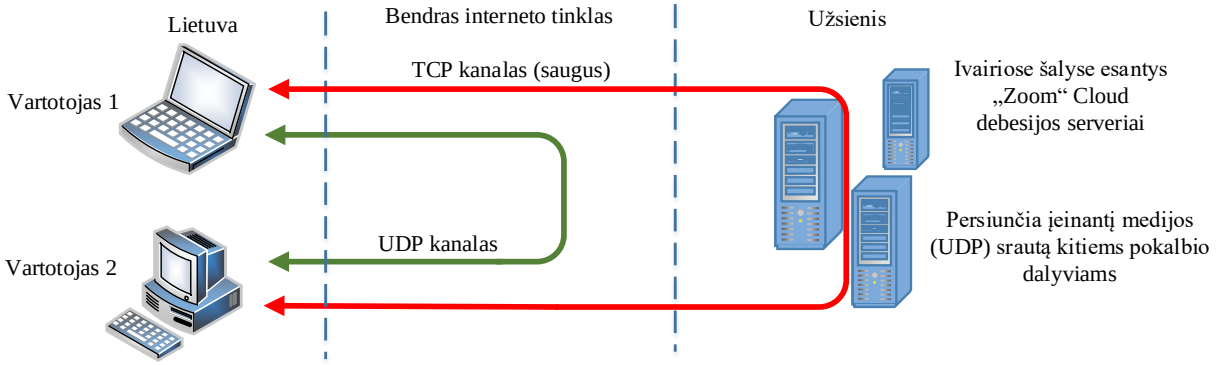
Mokamoje platformos versijoje galima kurti didesnius nei 1000 dalyvių, 24 val. trukmės sesijas palaikančius pokalbių kambarius, turinčius pildomas administravimo ir naudotojų valdymo, neriboto informacijos saugojimo, telefonijos ir kitas funkcijas [9].

TECHNINĖ „ZOOM“ SAUGUMO ANALIZĖ

Remiantis „Zoom“ dokumentacija, ryšys tarp vartotojų yra tiesiogiai šifruotas (*„End-to-End“* tipo), jo administravimas atliekamas įvairiose šalyse esančiuose „Zoom“ Cloud serveriuose [10], [11]. Mezgantis sesijai tarp dviejų vartotojų, „Zoom“ Cloud serveriai naudojami ryšio šifravimo raktų perdavimui. Apsikeitus šifravimo raktais, užmezgamas tiesioginis ryšys tarp vartotojų – informacija (sesijos vaizdas ir garsas) perduodama UDP kanalu, P2P (*angl.* Peer-to-peer) protokolu nenaudojant „Zoom“ Cloud serverių. Asociatyvi „Zoom“ veikimo schema esant dviem vartotojams pateikta 1 paveiksle. Dviejų vartotojų sesijos atveju TCP kanalu „Zoom“ Cloud serveriui perduodama tik sesijos statuso informacija, turiniu keičiamasi tiesiogiai tarp vartotojų.

Svarbus faktas yra tas, kad „Zoom“ produktų grupės vadovas (*angl.* Chief Product Officer) Oded Gal „Zoom“ portale patikslino, kad tiesioginio ryšio šifravimo principas

„End-to-End“ „Zoom“ platformoje taikomas ne visais atvejais. Patikslinimas iliustruotas aiškinamojo pobūdžio medžiaga [12]. Toronto universiteto tyrėjai nustatė, kad konferencijų metu šifravimo kodai buvo siunčiami per serverį, esantį Pekine [4].

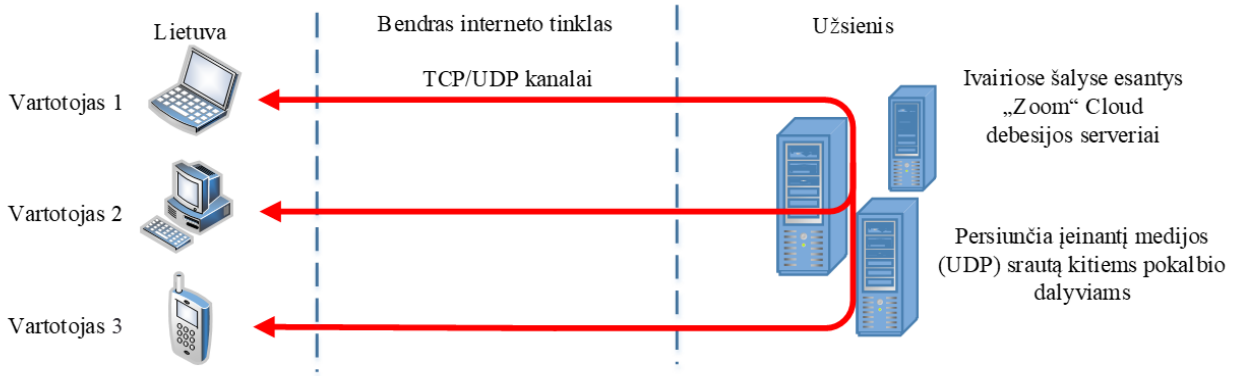


1 pav. „Zoom“ tinklo vaizdas ryšyje tarp 2 vartotojų. Pokalbis tarp vartotojų vykdomas tiesiogiai UDP kanalu, P2P protokolu, nenaudojant užsienyje esančių „Zoom“ Cloud serverių, šifruotai *„End-to-End“* principu [12]

Nustatyti 5 serveriai, esantys Kinijoje, ir 68 serveriai, esantys JAV, kurie, kaip manoma, veikia su tokia pačia programine įrangos versija. „Zoom“ neneigė turinti Kinijoje serverių, tačiau paminėjo, kad ji - ne vienintelė tokia JAV kompanija. Atsižvelgusi į spaudimą, „Zoom“ panaikino šifravimo kodų mainams naudotų Kinijoje esančių serverių funkcionalumą.

„Zoom“ pokalbių kambaryje dalyvaujant daugiau negu dviem vartotojams, visa informacija (sesijos vaizdas ir garsas, šifravimo raktai) siunčiami nutolusiems „Zoom“ Cloud serveriams. Iš jų informacija paskirstoma kiekvienam prie pokalbio prisijungusiam vartotojui – vartotojai sujungiami per bendrą interneto tinklą TCP/UDP kanalais. Principinė „Zoom“ platformos veikimo schema, esant daugiau negu dviem vartotojams, pateikta 2 paveiksle.

Priklausomai nuo to, ar pokalbių platformai pasiekti naudojama naršyklė, ar „Zoom“ klientas kompiuteryje, skiriasi naudojami ryšio šifravimo protokolai. Naršyklėje naudojamas simetrinio šifravimo protokolas AES-256-ECB, kompiuterio kliente – AES-128-ECB [13].



2 pav. „Zoom“ tinklo vaizdas tarp 3 ir daugiau vartotojų. Visa ryšio ir pokalbių informacija siunčiama per nutolusius „Zoom“ Cloud serverius [12]

AES yra laikomas saugiu algoritmu ir NIST savo rekomendacijose leidžia jo naudojimą [14], tačiau naudojamas ECB režimas turi esminių problemų – jis nėra semantiškai saugus ir šifruotas kanalas gali nutekinti informaciją [15].

Įvairių šaltinių duomenimis [[16] – [20], „Zoom“ turėjo spragų, keliančių susirūpinimą dėl asmeninės vartotojų informacijos saugumo. Viena iš jų – neautorizuoti vartotojai, sužinoję sesijos identifikacijos numerį (ID), galėjo prisijungti prie slaptažodžiu neapsaugotų pokalbių kambarių. Iki 100 ID per valandą buvo galima sužinoti panaudojus automatizuotą „Zoom“ ID skenavimo programą „zWarDial“, iki 2400 skirtingų ID per dieną [21]. Žinant susitikimo ID buvo galima sužinoti „Zoom“ pokalbio kambario nuorodą, datą ir laiką, susitikimo organizatorius ir temą.

Viena iš galimybių apsisaugoti nuo nepageidaujamų asmenų – naudoti atsitiktinai sugeneruotą susitikimo ID, ne tą patį ID kiekvienam susitikimui (kas yra populiaru tarp įprastų vartotojų). Taip pat, visiems dalyviams prisijungus, galima užrakinti susitikimą arba reikalauti iš kiekvieno prisijungiančiojo slaptažodžio [22].

2018 m. pabaigoje buvo nustatyta problema, susijusi su nuotolinio valdymo perdavimu [10]. Pažeidžiamumas leido neleistinai perimti kompiuterio pelės ir klaviatūros valdymą – vartotojui „Zoom“ platformoje pabendrinus periferijos valdymą, įsilaužėlis, žinantis tam tikrą sesijos informaciją, galėjo suformuoti specifinį tinklo paketą, kurį nusiuntus vartotojui būtų perimtas vartotojo periferijos valdymas. Būtina paminėti, kad šį pažeidžiamumą programinės įrangos kūrėjai pašalino, ir aprašytas neteisėtas nuotolinio perėmimo būdas, naudojantiems naujausią „Zoom“ versiją, nekelia grėsmės. Naujausia versija pasižymi papildomais saugumo elementais, suteikiančiais didesnį vartotojų privatumą – realizuota galimybė iš susitikimo pašalinti vartotoją, apriboti transliuojamą vaizdinę ir garsinę informaciją [22].

Tel. 1805
El. p. cert@nksc.lt
https://www.nksc.lt

„Zoom“ versijoje 4.6.11 (20559.0413) [24] buvo įgyvendintos saugumo pataisos – standartiniuose nustatymuose realizuota pokalbių kambarių apsauga slaptažodžiu, įvesta išorinių vartotojų indikacija, sugriežtintas pokalbių kambario administratoriaus priskyrimas. Plačiau naujos versijos funkcijos aprašomos „Zoom“ dokumentacijoje adresu: *https://support.zoom.us/hc/en-us/articles/201361953-New-Updates-for-Windows*.

„Zoom“ versijoje 5.0 buvo atsižvelgta į dar daugiau saugumo ir duomenų privatumo pažeidimų, todėl, esant poreikiui, NKSC rekomenduoja naudoti tik naujausią šios programinės įrangos versiją.

Tel. 1805
El. p. cert@nksc.lt
https://www.nksc.lt

ŠALTINIAI

[1] https://www.sec.gov/ix?doc=/Archives/edgar/data/1585521/000158552120000095/zm-20200131.htm
[2] https://www.nasdaq.com/market-activity/stocks/zm
[3] https://www.dgicommunications.com/technology/zoom-video-conferencing/
[4] https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings
[5] https://www.trustradius.com/products/zoom/reviews
[6] https://blogs.otago.ac.nz/zoom/zoom-on-mobile-devices/
[7] https://support.zoom.us/hc/en-us/articles/201362023-System-Requirements-for-PC-Mac-and-Linux
[8] https://zoom.us/download
[9] https://zoom.us/pricing
[10] https://medium.com/tenable-techblog/remotely-exploiting-zoom-meetings-5a811342ba1d
[11] https://citizenlab.ca/2020/04/faq-on-zoom-security-issues/
[12] https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/
[13] https://zoom.us/docs/doc/Zoom%20Encryption%20Whitepaper.pdf
[14] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175Br1.pdf
[15] https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Electronic_codebook_(ECB)
[16] https://time.com/5814981/zoom-videoconferencing-security-flaws-coronavirus/
[17] https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-zoom-ban-video-chat-privacy-security-a9456791.html
[18] https://www.newsweek.com/zoom-safe-privacy-risks-explained-video-calling-app-hacking-vulnerabilities-coronavirus-1495728
[19] https://www.bloomberg.com/news/articles/2020-04-07/taiwan-bans-government-use-of-zoom-over-cybersecurity-concerns
[20] https://time.com/5818851/spies-target-americans-zoom-others/
[21] https://www.theverge.com/2020/4/2/21206061/zoom-meeting-id-zwardial-automated-tool
[22] https://www.pocket-lint.com/apps/news/151603-what-is-zoombombing-how-to-stop-trolls-from-crashing-your-video-conference
[23] https://www.bbc.com/news/technology-52133349
[24] https://support.zoom.us/hc/en-us/articles/201361953-New-Updates-for-Windows