Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos

Regioninio kibernetinės gynybos centro

Tyrimų skyrius

„ACTi Corporation“ ir „GeoVision Inc“ gamintojų kamerų aparatinės ir programinės įrangos tyrimas

2025-05-26

Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos Regioninio kibernetinės gynybos centro tyrimų skyrius atliko „ACTi Corporation“ ir „GeoVision Inc“ gamintojų kamerų programinės įrangos kibernetinio saugumo tyrimą.

Tyrimo išvados:
Atlikus kamerų aparatinės ir programinės įrangos, RKGC tyrimų skyrius priėjo prie sekančių išvadų:

1. Kritinės spragos GeoVision kamerose. GeoVision GV-TBL4810 ir GV-EBD4813 kameros (programinė įranga V1.09, 2024-08-20) turi pažeidžiamumų (CVE-2024-11120, CVE-2024-6047, CVSS 9.8/10), leidžiančių nuotoliniu būdu vykdyti kodą ir visiškai perimti įrenginį be autentifikacijos;
2. GeoVision HTTP sąsajoje nėra autentifikacijos jautriems taškams (pvz., */config.xml*), todėl atskleidžiami konfigūracijos duomenys, keliantys riziką sekančioms atakoms vykdyti;
3. ACTi ActiveX pažeidžiamumai, ACTi A423 ir A77 kameros (programinė įranga A1D-506-S4.03.02-AC) naudoja pasenusias ActiveX valdymo priemones (CVE-2007-4583, CVE-2007-4582), leidžiančias vykdyti kodą ir manipuliuoti failais be autentifikacijos;
4. Nedokumentuoti prievadai, tiek GeoVision (prievadas 85), tiek ACTi (prievadai 6001, 6002, 20189) turi atvirus nedokumentuotus prievadus, kurie gali atverti kelią išnaudoti nežinomas paslaugas;
5. Saugus RTSP protokolas GeoVision kamerose, RTSP transliacija apsaugota „Digest“ autentifikacija, apsauganti nuo neteisėtos prieigos, tačiau tai nepašalina HTTP pažeidžiamumų.

Tyrimo rekomendacijos:

1. Atnaujinkite programinę įrangą nedelsiant. Reguliariai tikrinkite ir įdiekite naujausius atnaujinimus iš GeoVision ir ACTi svetainių, tokiu būdu ištaisytumėte žinomas spragas (pvz., CVE-2024-11120, CVE-2007-4583). Pakeiskite nepalaikomus įrenginius naujesniais modeliais;
2. Užtikrinkite stiprią autentifikaciją ir šifravimą. Įjunkite privalomą autentifikaciją visoms žiniatinklio sąsajoms (HTTP) ir naudokite HTTPS bei stiprius slaptažodžius ryšiui apsaugoti. ACTi atveju spręskite šifravimo silpnumo problemą pasirinkdami programinę įrangą su šiuolaikiniais kriptografiniais standartais;
3. Ribokite tinklo prieigą. Naudokite ugniasienės taisykles, kad apribotumėte prieigą prie kamerų prievadų (pvz., HTTP – 80, RTSP – 554) tik patikimiems IP adresams. Užblokuokite nedokumentuotus prievadus, kad sumažintumėte atakų paviršių;
4. Atskirkite kameras į atskirą VLAN. Kameras patalpinkite į dedikuotą VLAN, kad pažeidimo atveju užkirstumėte kelią prieigai prie kitų tinklo išteklių ir padidintumėte bendrą tinklo saugumą.

Turinys

1. Įžanga

Nacionalinis kibernetinio saugumo centras (NKSC) prie Krašto apsaugos ministerijos atsižvelgdamas į gautą UAB „Atea“ įmonės užklausos poreikį įvertinti vaizdo stebėjimo kamerų kibernetinį saugumą, atliko šių, gamintojų „ACTi Corporation“ ir „GeoVision Inc“, vaizdo stebėjimo kamerų vertinimą. Tyrimas atliktas nepriklausomai ir neįtakojus gamintojui, kai bendradarbiaujant su valstybės institucijomis, tyrimo objektai buvo gauti iš užsakovo UAB „Atea“.

Vaizdo stebėjimo sistemų gamintoja „Advanced Control & Technology Integration Corporation“ („ACTi Corporation“) yra Taivano korporacija, įsteigta 2003 m., turinti 400-500 darbuotojų [1], dirbanti su 100 pasaulio šalių, „ACTi Corporation“ sukurti produktai ir sprendimai yra plačiai naudojami dėl jų atitikties įvairiems saugumo reikalavimams, tokiems kaip „NDAA (National Defense Authorization Act)“, „TAICS (Taiwan Association of Information and Communication Standards)“, ir dėl prisitaikymo prie ypatingų vertikalių rinkų poreikių ir reikalavimų. [2], listinguojama Taivano vertybinių popierių biržoje [3]. Įmonė 2024 m. antrąjį ketvirtį „Product Matrix“ kataloge pristatė daugiau nei kelias dešimtis naujų ir įvairių konfigūracijų produktų – internetinių, giliojo mokymo kamerų ir jų sprendimų, termovizijos įrenginių, vidaus ir išorės stebėjimo kamerų, vaizdo glaudinimo ir transliavimo sprendimų, plataus funkcionalumo apsaugos kompleksų. „ACTi Corporation“ sprendimai orientuoti plačioms vartotojų grupėms – skirti naudoti pramonės, namų ūkių, valstybės institucijų paslaugų sferos sektoriuose, įmonės kuriamos technologijos taikytinos komercijos, eismo reguliavimo, bankininkystės, karo, švietimo, statybų, miesto priežiūros, apsaugos sistemų funkcionalumui užtikrinti [4]. Gamintojas vysto produktų plėtrą Europos Sąjungoje, gaminiai pristatomi tarptautinėse technologijų parodose ir konferencijose.

Kita tyrime nagrinėjama produkcija – gamintojo „GeoVision Inc“. „GeoVision Inc“ – Taivano įmonė, įkurta 1998 metais, veiklą vystanti vaizdo stebėjimo technologijų sektoriuje, listinguojama Taivano vertybinių popierių biržoje, turi 100-500 darbuotojų [5], produkciją tiekia daugiau nei į 110 šalių [6].

„ACTi Corporation“ ir „GeoVision Inc“ naudoja įvairius OEM (angl. Original Equipment Manufacturer) elektronikos komponentus, kurie gali atkeliauti ir iš Kinijos. Apie 30 kitų prekės ženklų bendradarbiauja su „ACTi Corporation“ įmone ir galimai naudoja vienas kito aparatinę įrangą, įskaitant tokia įmones kaip „GeoVision Inc“ [7], „HIKVISION“ [8], „Dahua“ [9], gali papildomai įrašyti savo programinę įrangą ir taip toliau platinti su savo prekės ženklu. Atskirai verta paminėi, jog kompanija „GeoVision Inc“ tikrai naudoja „ACTi Corporation“ įmonės programinę įrangą (VMS) [10].

Tyrimo imtyje nagrinėti įrenginiai – Lietuvoje platinamos teritorijų stebėjimui skirtos kameros – „ACTi Corporation“ vaizdo stebėjimo kameros „A423-00AXX-24A-0259“, „A77-00AXXX-24E-0497“ ir „GeoVision Inc“ vaizdo stebėjimo kameros „GV-TBL4810“, „GV-EBD4813“. Tyrime dalyvavusios produkcijos vaizdai patekti 1 paveiksle.

1 pav. Tyrime dalyvavusios „ACTi Corporation“ ir „GeoVision Inc“ produkcijos vaizdai

„ACTi Corporation“ kamera „A423-00AXX-24A-0259“ – lauko sąlygomis skirtas naudoti įrenginys, turintis išorinę linzę, 6MP rezoliucijos, palaikantis H.265+ audiovizialinio turinio glaudinimo technologiją [11]. Kamera „A77-00AXXX-24E-0497“ – lauko sąlygomis skirtas naudoti įrenginys, turintis išorinę linzę, 6MP rezoliucijos, palaikantis H.265+ audiovizialinio turinio glaudinimo technologiją [12]. „GeoVision Inc“ kamera „GV-TBL4810“ – išorės stebėjimui, valdoma kamera, turinti 4MP kamera, bei gilaus mokymosi funkcija pasitelkiant DI (Dirbtini Intelektą), palaikantį audiovizualinio turinio glaudinimo H.265, H.264 arba MJPEG

formatus.[13]. Kamera „GV-EBD4813“ – išorės stebėjimui, valdoma kamera, turinti 4MP kamera, bei gilaus mokymosi funkcija pasitelkiant DI, palaikantį audiovizualinio turinio glaudinimo H.265, H.264 arba MJPEG formatus.[14]. Kameros gaminamos nuo 2021 m.

Tyrime buvo atliekami veiksmai ir jų seka taip, kad kiti tyrėjai galėtų atkartoti NKSC analizės rezultatus ir turėtų gauti analogiškus rezultatus. Tyrimo metodika paremta:

1) programinės įrangos funkcionalumo analize;
2) kamerų kuriamų duomenų srautų struktūros ir turinio analizė;
3) aparatinės dalies ir elektronikos komponentų dekompozicija.

Aparatinės dalies tyrimo metu buvo atlikta įrenginiuose naudojamų mikroschemų atitikties analizė, įvertinta gaminio schemotechninė struktūra ir jo pagaminimo kokybė. Šiame tyrime įrenginiai buvo demontuoti iki ribos, kurią peržengus atgalinis surinkimas būtų galimas tik panaudojus precizinę įlitavimo / išlitavimo įrangą, tokiu atveju padidinant riziką negrįžtamai dėl proceso metu naudojamos aukštos temperatūros pažeisti mikrograndynuose esamą informaciją.

2. Žinomų pažeidžiamumų analizė

Atlikus „ACTi Corporation“ ir „GeoVision Inc“ stebėjimo kamerų dekompozicijos tyrimą nustatyta, kad 2021 m. ir 2024 m. pagamintose „GeoVision Inc“ kamerose yra naudojami programiniai sprendimai, parengti 2023 – 2024 m. laikotarpiu, turintys žinomų kibernetinio saugumo spragų, pažymėtų viešai prieinamoje pažeidžiamumų duomenų bazėje (angl. Common Vulnerabilities and Exposures – CVE). Buvo nustatyti kamerose įdiegti programiniai paketai, turintys CVE žemiau pateiktus pažeidžiamumus ir abiejų pažeidžiamumų grėsmingumo balas yra salyginai aukštas. Nustatyti pažeidžiamumai įgalina kameros informacijos perėmimą nuotoliniu būdu, žalingo kodo įvykdymą. Taip pat užpuolikai gali modifikuoti įrenginio prisijungimo atsaką, kad apeitų autentifikavimą ir gautų neteisėtą prieigą prie žiniatinklio programos.. Tirti tie programinio kodo paketai, kurie naudoti tirtuose pavyzdžiuose ir įdiegti įsigytose kamerose (angl. Out of the box).

“ GeoVision Inc“ GV-TBL4810 ir GV-EBD4813 programinės įrangos versija V1.09 2024-08-20. Programinė įranga V1.09, išleista 2024 m. rugpjūčio 20 d., turi kelis bendruosius pažeidžiamumus ir grėsmes (CVE). Čia pateikiami keli svarbiausi:

1. CVE-2024-11120 — OS komandų įterpimas GeoVision pabaigos ciklo įrenginiuose. Šis pažeidžiamumas leidžia neautentifikuotam nuotoliniam užpuolikui įterpti bet kokias operacinės sistemos komandas į įrenginį. Tai vyksta dėl netinkamo įvesties patikrinimo, kai įrenginys nefiltruoja duomenų, naudojamų sistemos komandose, todėl įvyksta komandų įterpimas. Galimas nuotolinis kodo vykdymas, užpuolikas gali vykdyti bet kokią komandą įrenginyje — kurti užpakalinius vartus, vogti duomenis arba trikdyti įrenginio veikimą. Taip pat užpuolikas įgyja pilną kamerų valdymą — gali manipuliuoti vaizdo srautu, išjungti saugumo įspėjimus arba naudoti įrenginį kaip vartus į kitus tinklo resursus. Pažeidžiamumo vertinimas yra **kritinis** (CVSS 9.8/10) — itin pavojinga, nes užpuolikui nereikia jokios autentifikacijos ar specialių teisių, todėl lengvai panaudojama nuotoliniu būdu.
2. CVE-2024-6047 — netinkamas įvesties tikrinimas, leidžiantis vykdyti bet kokį kodą. Kai kurie GeoVision įrenginiai netinkamai tikrina įvesties parametrus, leidžiant užpuolikams įterpti kenksmingas komandas, kurios sukelia bet kokio kodo vykdymą įrenginyje. Galimas pilnas įrenginio užgrobimas, užpuolikai gali vykdyti bet kokį kodą kameroje, įskaitant kenkėjiškų programų įdiegimą ar vaizdo srauto šnipinėjimą. Taip pat galimas tinklo perėmimas, užkrėstos kameros gali būti naudojamos tolimesniems išpuoliams prieš vidinį tinklą. Pažeidžiamumo vertinimas yra **kritinis** (CVSS 9.8/10) — labai rimtas, nes gali būti išnaudojamas nuotoliniu būdu be prisijungimo.
3. CVE-2009-5087 — katalogų perėjimas GeoVision geohttpserver serveryje. Užpuolikai gali naudoti katalogų perėjimo techniką (pvz., "../" URL adresuose), kad pasiektų failus už leidžiamos interneto direktorijos ribų, taip potencialiai atskleisdami jautrius failus. Galimas informacijos nutekėjimas, užpuolikai gali perskaityti konfigūracijos failus, slaptažodžius ar kitus įrenginyje saugomus jautrius duomenis. Taip pat galima vykdyti žvalgyba, surinkta informacija gali padėti planuoti tolimesnius išpuolius arba teisės suteikimą. Pažeidžiamumo vertinimas yra **vidutinis** — nors tiesiogiai nekoduojamas kodo vykdymas, informacijos nutekėjimas gali lemti rimtesnius išpuolius.

4. CVE-2009-1092 — (angl. Use after free) pažeidžiamumas LiveAudio ActiveX valdiklyje. Use after free klaida ActiveX valdiklyje leidžia užpuolikams vykdyti bet kokį kodą manipuliuojant garso funkcijomis GeoVision DVR sistemose. Galimi padariniai — nuotolinis kodo vykdymas, užpuolikas gali paleisti kenksmingą kodą sistemoje, kur veikia pažeidžiamas valdiklis, galimai užvaldydamas visą sistemą. Gali sukelti sistemos avarijas arba paslaugos nepasiekiamumą. Pažeidžiamumo vertinimas yra **aukštas** — reikalauja naudotojo įsikišimo, tačiau gali sukelti pilną sistemos užgrobimą.
5. CVE-2005-1553 — silpnas slaptažodžių šifravimas. Senoji GeoVision programinė įranga naudojo silpną šifravimą slaptažodžiams apsaugoti, todėl užpuolikai galėjo perimti tinklo srautą ir atkurti slaptažodžius. Galimybė vykdyti tapatybės vagyste, užpuolikai gali pagauti ir pavogti vartotojo prisijungimo duomenis, įgydami neteisėtą prieigą. Taip pat vykdyti neteisėta prieiga, su pavogtais slaptažodžiais užpuolikai gali valdyti kameras ar DVR sistemas. Pažeidžiamumo vertinimas yra **aukštas** — nors ir pasenęs, kelia didelį pavojų, jei naudojami seni įrenginiai ar programinė įranga.
6. CVE-2004-2101 — buferio perpildymas, sukeliantis paslaugos nutraukimą (DoS). Buferio perpildymas sysinfo skripte leidžia užpuolikams siųsti specialiai paruoštą užklausą, kuri gali sukelti įrenginio arba paslaugos gedimą. Nustatyti galimi padariniai yra paslaugos nutraukimas, kuomet įrenginys arba paslauga sugenda, trikdydama stebėjimą. Galimas kodo vykdymas, nors daugiausia DoS, kartais buferio perpildymas gali būti išnaudotas kodo vykdymui. Pažeidžiamumo vertinimas yra **vidutinis** — daugiausia trikdo veikimą, tačiau gali būti išnaudotas toliau.
7. CVE-2004-2100 — autentifikacijos apeinimas naudojant URL kodavimą. Užpuolikai gali apeiti autentifikaciją, išnaudodami netinkamą URL koduotų naujų eilučių simbolių tvarkymą, gaudami neteisėtą prieigą prie ribotų zonų. Galimi padariniai susiję su neteisėta prieiga, užpuolikai gali matyti arba valdyti ribotus duomenis ar funkcijas be prisijungimo. Vykdyti informacijos nutekėjima, gali atskleisti jautrią informaciją. Pažeidžiamumo vertinimas yra **vidutinis** — pažeidžia prieigos kontrolę, bet tiesiogiai neleidžia vykdyti kodo.

Įvertinus rizikas, kritiniai pažeidžiamumai yra (CVE-2024-11120, CVE-2024-6047), kurie kelia itin didelį pavojų dėl galimybės nuotoliniu būdu vykdyti kenkėjišką kodą be autentifikacijos. Tai gali lemti pilną įrenginio užgrobimą ir tinklo kompromitavimą.

Aukšto lygio pažeidžiamumai (CVE-2009-1092, CVE-2005-1553) yra vis dar reikšmingi, ypač jei reikalingas naudotojo įsikišimas arba naudojami seni įrenginiai.

Vidutinio lygio pažeidžiamumai (CVE-2009-5087, CVE-2004-2101, CVE-2004-2100), dažniausiai veikia konfidencialumą ir prieinamumą, bet gali būti naudojamos kaip pagrindas rimtesniems išpuoliams.

"ACTi Corporation" A423 ir A77 programinės įrangos versija A1D-506-S4.03.02-AC, ACTi kameros turi keletą saugumo pažeidžiamumų:

1. CVE-2007-4583 — ActiveX pažeidžiamumas valdiklyje. Šis pažeidžiamumas susijęs su „nvUtility.Utility.1" ActiveX valdikliu, kuris leidžia įvesti failo kelią. Tačiau valdiklis netinkamai tikrina vartotojo pateiktą kelią, todėl užpuolikas gali nurodyti pilną failo kelią ir sukurti arba perrašyti failus sistemoje. Ši klaida buvo atskleista saugumo tyrimų metu, kuomet analizuotos ActiveX komponentų galimybės įtakotų failų sistemą. Šis pažeidžiamumas sudaro galimybe tiesiogiai kurti ar keisti failus:
    a. Įrašyti kenkėjišką kodą į įrenginio failų sistemą;
    b. Pakeisti svarbius konfigūracijos failus, trikdant įrenginio veikimą;
    c. Gauti tolimesnę prieigą prie sistemos, išnaudojant kitus silpnumus;
    d. Nuotolinis įrenginio užgrobimas;
    e. Duomenų praradimas ar pakeitimas;
    f. Prarandama sistemos kontrolė ir saugumo garantijos;

    Pažeidžiamumo vertinimas yra **kritinis**, kadangi veikia nuotoliniu būdu, net nereikalaujant prisijungimo;

2. CVE-2007-4582 — buferio perpildymo pažeidžiamumas ActiveX valdiklyje. Ši klaida randama „nvUnifiedControl.AUnifiedControl.1“ ActiveX valdiklyje, kur funkcija „SetText“ priima du parametrus. Jei antrasis parametras yra pernelyg ilgas, gali įvykti buferio perpildymas, leidžiantis vykdyti savavališką kodą. Atliekant saugumo testavimus ir kodo analizę buvo nustatyta, kad nėra pakankamai tikrinamas įvesties ilgis, o tai sukelia atminties perkrovą. Buferio perpildymas yra viena iš populiariausių pažeidžiamybių, nes leidžia užpuolikams:
    a. Įvykdyti savo kodą sistemoje;
    b. Užgrobti įrenginį arba gauti aukštesnes privilegijas;
    c. Įdiegti kenkėjiškas programas ar pakeisti įrenginio elgseną.

    Galimi padariniai:
    d. Pilnas įrenginio perėmimas;
    e. Įrenginio veikimo sutrikimai ar perėmimas;
    f. Tinklo saugumo pažeidimai per užkrėstą įrenginį.

Pažeidžiamumo vertinimas yra **kritinis**, kadangi galima nuotoliniu būdu vykdyti kodą be autentifikacijos.

3. VU#355151 — daugialypiai pažeidžiamumai A1D-500-V6.11.31-AC programinėje įrangoje. Šiame įrenginių modelyje ir programinės įrangos versijoje nustatyti keli skirtingi pažeidžiamumai:
    a. CVE-2017-3184, netinkama autentifikacija leidžia neautorizuotiems vartotojams pasiekti kritines funkcijas, tokias kaip gamyklinių nustatymų atstatymas;
    b. CVE-2017-3185, informacijos atskleidimas per GET užklausas, leidžiantis gauti konfigūracijos ar kitus jautrius duomenis;
    c. CVE-2017-3186, silpni slaptažodžių reikalavimai ir numatytieji slaptažodžiai, kurie lengvai išgaunami arba atspėjami.

    Atliekant tinklo saugumo auditą ir bandymus išnaudoti silpnąsias vietas, buvo nustatyta, kad įrenginys neužtikrina tinkamos prieigos kontrolės. Šie pažeidžiamumai leidžia užpuolikams:
    a. Nuotoliniu būdu pakeisti kameros nustatymus, iš naujo ją paleisti ar ištrinti konfigūraciją;
    b. Gauti slaptus duomenis, pavyzdžiui, vartotojų prisijungimus;

c. Lengvai patekti į sistemą dėl silpnų slaptažodžių;
d. Saugumo kontrolės praradimas;
e. Įrenginio visiškas užgrobimas;
f. Tolimesni išpuoliai prieš vidinį tinklą per kompromituotą kamerą.

Pažeidžiamumo vertinimas yra nuo **vidutinio** iki **aukšto**, priklausomai nuo to, kiek įrenginyje yra naudojama apsaugų ir kaip įrenginys yra sukonfigūruotas ir naudojamas.

Bendras pažeidžiamumų šiai kamerai kontekstas yra pavojingas, ACTi kamerų pažeidžiamumai dažnai kyla dėl senų programinės įrangos komponentų, ypač ActiveX valdiklių, kurie turi daug saugumo spragų. Dėl to nuotolinis kodų vykdymas — leidžia užpuolikams nuotoliniu būdu įsilaužti į įrenginį, neturint jokių prisijungimo duomenų. Taip pat egzistuoja sistemos valdymo praradimas, kuomet užvaldžius kamerą galima manipuliuoti stebėjima, išjungti signalizacijas arba naudoti įrenginį kaip vidinės atakos šaltinį. Kuomet yra galimas duomenų nutekėjimas, leidžiantis gauti konfigūracijos failus, slaptažodžius ar kitą jautrią informaciją.

Visi šie veiksniai daro ACTi kameras pažeidžiamas ir potencialiai pavojingas infrastruktūros taškus, ypač jei jos naudojamos verslo ar saugumo sistemose.

3. „GeoVision Inc“ kamerų dinaminė analizė

Šis vertinimas buvo skirtas išsamiai patikrinti GeoVision GV-TBL4810 saugumą, ypač atsižvelgiant į įprastas atakas HTTP ir RTSP paslaugoms, autentifikacijos mechanizmams, programinės įrangos pažeidžiamumus ir žinomus viešus CVE, tokius kaip CVE-2024-6047 ir CVE-2024-11120. Testavimas atskleidė kritines spragas, ypač neužtikrintą HTTP sąsają, leidžiančią atakutojams be autentifikacijos pasiekti jautrius galinius taškus, pvz., */config.xml* ir pagrindinę administracinę sąsają */page/common/index_ipc.13c4a21a.htm*.

Kita vertus, RTSP srautinio perdavimo paslauga nustatyta saugi, naudodama „Digest„ autentifikaciją, kuri tinkamai blokuoja neautorizuotą prieigą. Nors testavimo metu nebuvo patvirtintų pažeidžiamumų, susijusių su žinomais CVE, programinės įrangos versijos informacijos trūkumas ir išliekantys HTTP saugumo trūkumai kelia pavojų.

Siekiant sumažinti šias rizikas, griežtai rekomenduojami neatidėliotini veiksmai – gamyklinis atstatymas ir programinės įrangos atnaujinimas. Ši ataskaita pateikia išvadas,

įrodomuosius pavyzdžius (PoC), aptaria eksploatavimo rizikas ir siūlo konkrečias pataisos priemones.

GeoVision įrenginių ankstesnės spragos

GeoVision prietaisai turi istoriją kritinių pažeidžiamumų, įskaitant neautentifikuotą nuotolinį kodų vykdymą per backdoor ir buferio perpildymus, kurie kai kuriose senose versijose nebuvo pataisyti. Istoriniai pažeidžiamumai:

1. 2017 m. root prieiga per paprastą HTTP komandą;
2. Hardcode root slaptažodžiai ir SSH/HTTPS raktai;
3. 2023 m. spragos leidusios neautorizuotą prieigą prie web sąsajos.

Jei GV-TBL4810 naudoja pasenusią programinę įrangą, šios spragos gali būti aktyvios:

1. Eksploatavimo scenarijai
2. Neautorizuota konfigūracijos prieiga.
3. CVE pažeidžiamumų išnaudojimas nuotoliniam kodų vykdymui.
4. Slaptažodžių vagystė per senas spragas.
5. Sumažinimo priemonės

Testavimo metodika

Testavimas vyko derinant automatizuotus ir rankinius metodus, siekiant atrasti galimas saugumo spragas kameros apsaugoje. Buvo naudojami specialūs Python prograiniai kodai, automatizuojantys galinių taškų patikrinimus, o taip pat rankiniai įrankiai – curl komandos, ffplay media analizatorius (RTSP srautui) ir tinklo įrankiai, tokie kaip netcat, leidžiantys imituoti įvairias atakos strategijas. Testavimo etapai buvo:

1. Galinių taškų nustatymas: HTTP ir RTSP sąsajų skenavimas, siekiant identifikuoti pasiekiamus galinius taškus ir patikrinti autentifikacijos poreikį;
2. Įvesties validacija: siunčiant neteisingus ar neįprastus HTTP ir RTSP užklausas, stebint kameros reakciją į neįprastus duomenis;
3. Parametrų klastojimas: bandymai manipuliuoti URL parametrais ir slapukais siekiant apeiti prieigos kontrolę.
4. Metodų ir antraščių testavimas: įvairių HTTP metodų ir antraščių apdorojimo analizė;
5. CVE imitavimas: bandymai išnaudoti viešai žinomus pažeidžiamumus, ypač CVE-2024-6047, leidžiantį nuotolinį kodo vykdymą;

6. Autentifikacijos tikrinimas: tikrinamas autentifikacijos mechanizmų veiksmingumas HTTP ir RTSP paslaugose

Nustatyta, kad GeoVision GV-TBL4810 neužtikrinta HTTP sąsaja. Nereikalaujama jokia autentifikacija prie galinių taškų (angl. key endpoint), tokių kaip */config.xml*, kuriame yra konfigūracijos duomenys, arba administracinės sąsajos */page/common/index_ipc.13c4a21a.htm*. atliemant įprasta „curl“ operacija gaunamas atsakas: *<!DOCTYPE html><html><head><title></title><META http-equiv="Content-Type" content="text/html;charset=utf-8"><META http-equiv="Pragma" content="no-cache"><META http-equiv="Cache-Control" content="no-cache"><META http-equiv="Expires" content="0"><style type="text/css">html, body{height: 100%;margin: 0px;overflow: hidden;}</style><script type="text/javascript">function release(){document.frames['banner'].release();}</script></head><body><iframe name="banner" id="banner" hideFocus="hideFocus" marginwidth="0" marginheight="0" src="../index.htm?clientIpAddr=192.168.1.122&IsRemote=0" frameborder="0" width="100%" height="100%"></iframe></body></html>*

Pagrindinis HTTP taškas grąžina HTML puslapį, kuris įkelia */index.htm* per iframe be prisijungimo*, /index.htm* nukreipia į administracinę sąsają, prieinamą be autentifikacijos. Taip pat nustatyta, kad /config.xml atiduoda konfigūracijos duomenis bet kam tinkle. Nors ši informacija nėra kritinė, tačiau išduoda konfigūracijos pasirinktis kurios galėtų buti pardinis taškas tolesniam atakos vektoriui.

Ši spraga yra kritinė, kadangi leidžia bet kam tinkle pasiekti konfigūraciją ir galbūt keisti svarbius nustatymus, pvz., išjungti AI funkcijas, pakeisti srauto paskyras ar tinklo konfigūraciją. Atsižvelgiant į GeoVision ankstesnius saugumo incidentus, ši neužtikrinta sąsaja kelia rimtą pavojų. Bandymų pavyzdžiai:

```
curl http://192.168.1.223/config.xml  # Konfigūracija be autentifikacijos
curl http://192.168.1.223/page/common/index_ipc.13c4a21a.htm  # Administracinė sąsaja
```

Nustatyta, kad manipuliacijos su URL parametrais (pvz., admin=1) arba slapukais neturi poveikio. Bandymas prisijungti per */login* baigiasi 404 klaida.

Tyrimo metu ištirta saugi RTSP srauto paslauga su Digest autentifikacija. RTSP srautai (554 ir 8554 prievadai) apsaugoti Digest autentifikacija, kuri tikrina teisingus prisijungimus. Bandymų metu neautentifikuotos užklausos buvo atmetamos su 401 klaida. Paslauga atspari neteisingiems duomenims ir nepalaikomiems metodams. Netinkamos RTSP komandos grąžino 401 klaidą, nesukeldamos klaidų ar duomenų nutekėjimo. Taigi nustatyta, kad Digest

autentifikacija reikalauja galiojančių duomenų prieš leidžiant srautą. Žemiau pavyzdys kuris nurodo tinakma autentifikacijos buvimą:

```
printf "DESCRIBE rtsp://192.168.1.223:554/CH001.sdp RTSP/1.0\r\nCSeq: 1\r\n\r\n" | nc 192.168.1.223 554  # Laukiama 401 klaida
```

Galimos programinės įrangos spragos (CVE-2024-6047, CVE-2024-11120). Testavimo metu kameros programinės įrangos versija nenustatyta. Žinomi pažeidžiamumai leidžia nuotolinį kodą vykdyti su aukštu pavojingumo balu (9.8). Bandant prieiti prie */cgi-bin/admin* su specialiai paruoštomis antraštėmis, gauta 404 klaida, tad šie galiniai taškai gali būti pataisyti arba pašalinti. Nepaisant to, neužtikrinta HTTP sąsaja padidina bendrą atakos paviršių. Žemiau išbandyta prieiga:

```
curl -H "X-Command: exec" "http://192.168.1.223/cgi-bin/admin?cmd=id"  # Laukiama 404 klaida
```

HTTP įvesties apdorojimas ir stabilumas

Nepaisant autentifikacijos spragų, HTTP serveris stabilus ir nepraranda jautrumo į neteisingas užklausas ar nepalaikomus metodus. Serveris priima URL parametrus be validacijos, kas gali būti rizikinga kartu su kitomis spragomis. Testai su kenksmingomis antraštėmis (pvz., JavaScript) neparodė XSS pažeidžiamumo.

3.1. Prievadų skenavimas ir įrenginio matomumo analizė

Atliktas išsamus GeoVision IP kamerų prievadų skenavimas bei įrenginio sistemos identifikavimo bandymas naudojant prievadų analizės metodus. Šio proceso tikslas buvo nustatyti, kokios tinklo paslaugos aktyvios įrenginyje, kaip kamera save pateikia tinklo aplinkoje ir ar yra atvirų prievadų, kurie gali reikšti galimus saugumo pažeidimus ar nenumatytas prieigas. Pradinis skenavimas atliktas nustatyti ne tik atvirus TCP prievadus, bet ir identifikuoti veikiančias paslaugas bei operacinės sistemos tipą. Gauti rezultatai atskleidė atvirus šiuos prievadus:

1. 80 (HTTP – naudojamas web sąsajai);
2. 81 (tikėtina SOAP/ONVIF sąsaja);
3. 85 (GV-EBD4813 neidentifikuota paslauga);
4. 554 (RTSP – video transliacija);

Analizuojant kameros web sąsają, buvo nustatyta, kokie prievadai yra pateikiami naudotojo GUI aplinkoje ir kaip tai atitinka realią situaciją tinklo lygyje. Web sąsajoje matomi aukščiau nurodyti prievadai. Tačiau prievadų analizė parodė papildomą – 85 prievadą, kuris sąsajoje neminimas. Tai leidžia daryti prielaidą, kad šis prievadas nėra skirtas vartotojo sąveikai, o gali būti skirtas vidiniam įrenginio valdymui, debug funkcijoms arba išvis būti atsitiktinai paliktas atviras. Prievadai, kurie nėra dokumentuoti, dažnai tampa silpnąja sistemos vieta – nesaugomi, neregistruojami, o todėl ir nepastebimi saugumo stebėsenos metu.

Abi Geovision kameros identifikuotos kaip veikiančios Linux pagrindu, o tai leidžia daryti prielaidą apie atvirą operacinės sistemos architektūrą, galimai su papildomomis paslėptomis funkcijomis ar įrankiais.

3.2. HTTP sąveika su SOAP (ONVIF) sąsaja

Siekiant ištirti, ar ONVIF protokolas tinkamai įdiegtas ir prieinamas per 81 prievadą, atlikta HTTP sąveikos analizė naudojant paprastą GET metodo užklausą per *curl* įrankį: *curl http://192.168.1.32:81.* Tikėtasi gauti arba XML struktūrą (reiškiančią atsakymą į SOAP užklausą), arba bent HTTP protokolo atsakymą, rodantį sąsajos veikimą. Gautas atsakymas „HTTP GET method not implemented“ rodo, kad sąsaja reaguoja į HTTP užklausas, tačiau priima tik POST metodą, kas atitinka ONVIF SOAP specifikaciją. Tai leidžia daryti išvadą, kad kamera elgiasi korektiškai pagal standartą, neatsako į netinkamus užklausų tipus, o tai rodo sąsajos stabilumą ir tam tikrą saugumo lygį. Be to, šis atsakas reiškia, kad sistema negali būti išnaudota per paprastus HTTP GET metodus, kas yra dažnas bandymas išnaudoti web serviso pažeidžiamumus. Pilnas atsakas pateikiamas žemiau:

```
<?xml version="1.0" encoding="UTF-8"?>

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xop="http://www.w3.org/2004/08/xop/include"
xmlns:xmime4="http://www.w3.org/2004/11/xmlmime"
xmlns:wsa5="http://www.w3.org/2005/08/addressing" xmlns:wsrf-bf="http://docs.oasis-
open.org/wsrf/bf-2" xmlns:wstop="http://docs.oasis-open.org/wsn/t-1" xmlns:wsrf-
r="http://docs.oasis-open.org/wsrf/r-2" xmlns:tes-
e="http://www.onvif.org/ver10/events/wsdl/EventBinding"
xmlns:tev="http://www.onvif.org/ver10/events/wsdl" xmlns:tes-
nc="http://www.onvif.org/ver10/events/wsdl/NotificationConsumerBinding" xmlns:tes-
np="http://www.onvif.org/ver10/events/wsdl/NotificationProducerBinding" xmlns:tes-
```

```
sm="http://www.onvif.org/ver10/events/wsdl/SubscriptionManagerBinding"
xmlns:tns1="http://www.onvif.org/ver10/topics"
xmlns:xmime="http://www.w3.org/2004/06/xmlmime"
xmlns:tt="http://www.onvif.org/ver10/schema" xmlns:wsnt="http://docs.oasis-
open.org/wsn/b-2" xmlns:tds="http://www.onvif.org/ver10/device/wsdl"
xmlns:timg="http://www.onvif.org/ver20/imaging/wsdl"
xmlns:tmd="http://www.onvif.org/ver10/deviceIO/wsdl"
xmlns:tptz="http://www.onvif.org/ver20/ptz/wsdl"
xmlns:trt="http://www.onvif.org/ver10/media/wsdl"
xmlns:tr2="http://www.onvif.org/ver20/media/wsdl" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" xmlns:ter="http://www.onvif.org/ver10/error"
xmlns:tan="http://www.onvif.org/ver20/analytics/wsdl" xmlns:tan-
ae="http://www.onvif.org/ver20/analytics/wsdl/AnalyticsEngineBinding" xmlns:tan-
re="http://www.onvif.org/ver20/analytics/wsdl/RuleEngineBinding"
xmlns:trc="http://www.onvif.org/ver10/recording/wsdl"
xmlns:trp="http://www.onvif.org/ver10/replay/wsdl"
xmlns:tse="http://www.onvif.org/ver10/search/wsdl"
xmlns:tpl="http://www.onvif.org/ver10/plus/wsdl"
xmlns:tplt="http://www.onvif.org/ver10/plus/schema" xmlns:ns1="GenetecPtzPatterns"
xmlns:tpv="http://www.onvif.org/ver10/provisioning/wsdl"><SOAP-ENV:Body><SOAP-
ENV:Fault><faultcode>SOAP-ENV:Client</faultcode><faultstring>HTTP GET method not
implemented</faultstring></SOAP-ENV:Fault></SOAP-ENV:Body></SOAP-ENV:Envelope>↵
```

Atlikta analizė patikrinant ONVIF funkcionalumą, sukomponuotas Python pagrindu kodas, pasitelkiant biblioteką *onvif-zeep*, pavyzdys pateiktas žemiau:

```
from onvif import ONVIFCamera
      cam = ONVIFCamera('192.168.1.32', 81, 'admin', 'Kamera1234')
      media_service = cam.create_media_service()
      profiles = media_service.GetProfiles()
      for profile in profiles:
          print(profile)
```

Tikslas – gauti medijos profilius, kuriuose aprašytos transliacijos charakteristikos. Kodas prisijungė prie kameros per 81 prievadą, autentifikavosi naudotojo vardu ir slaptažodžiu, inicijavo SOAP sesiją ir gavo atsakymus su transliacijos parametrais. Rezultatai parodė, kad kamera palaiko transliaciją 2688x1520 raiška, H264 vaizdo kodeku bei G711 audio suspaudimu. Tai rodo, kad įrenginys visiškai palaiko ONVIF standartus ir gali būti integruojamas į stebėjimo sistemas. Toks funkcionalumas taip pat gali būti potencialus pažeidžiamumo šaltinis, jei ONVIF prieiga neapsaugota tinkamais slaptažodžiais, sertifikatais ar kitais autentifikavimo metodais.

3.3. Nedokumentuoto prievado analizė

Kadangi 85 prievado paskirtis nebuvo žinoma, atlikti išsamūs tyrimai pasitelkiant tiek aktyvius, tiek pasyvius metodus. Naudotas įrankis *netcat*, siunčiant paprastą tekstinę užklausą:

```
echo -e "HELLO\r\n\r\n" | nc 192.168.1.32 85,
```

Tačiau atsakymo negauta. Tai gali reikšti, kad paslauga pasyvi arba reaguoja tik į specifinį protokolą. Papildomai atliktas versijos identifikavimo bandymas su `-sV` opcija, tačiau rezultatas grąžino „mit-ml-dev?“, kas gali reikšti nestandartinį servisą, eksperimentinį modulį ar uždarą, dokumentacijoje neminimą protokolą. Tokie neidentifikuoti prievadai vertinami kaip galimai pažeidžiami, nes jų funkcionalumas nėra žinomas, jie gali būti neapsaugoti slaptažodžiais ar autentifikacija, ir yra nematomi standartiniams saugumo įrankiams.

3.4. Pažeidžiamumų skenavimas

Siekiant nustatyti, ar kamera turi žinomų pažeidžiamumų, atliktas automatizuotas scenarijų skenavimas su `--script vuln` parametrais. Šis metodas leidžia aptikti žinomas CVE spragas, kurios gali būti aktyvios aptariamame įrenginyje. Nustatyta, kad kamera pažeidžiama „Slowloris“ tipo atakai (CVE-2007-6750), kurios metu HTTP serveris gali būti išnaudojamas laikant atviras jungtis su neišbaigtomis antraštėmis. Tai leidžia susieti serverio resursus ir sukelti paslaugų trikdymą (DoS). Nors ši pažeidžiamumo rūšis nėra skirta nuotoliniam kodų vykdymui, ji vis tiek gali būti reikšminga organizacijoms, kurioms svarbus nepertraukiamas vaizdo transliavimas. Kitų reikšmingų ar lengvai išnaudojamų spragų nustatyta nebuvo.

3.5. CGI prieigų patikra

Siekiant išsiaiškinti, ar kamera palaiko */cgi-bin/* tipo struktūras, dažnai naudojamas IP kamerose, atlikti automatizuoti užklausų testai su dažniausiai pasitaikančiais keliais *(angl. Paths),* pavyzdžiui vieni iš jų.:

1. `/cgi-bin/snapshot.cgi`;
2. `/cgi-bin/video.cgi`;
3. `/cgi-bin/admin.cgi`.

Bandymuose naudotas `curl` su autentifikacija: `curl -u admin:Kamera1234`. Visi atsakymai buvo 404 tipo klaidos, rodančios, kad šie keliai neegzistuoja. Tai gali reikšti, kad CGI struktūra arba išvis nenaudojama, arba yra perkeliama į kitą sisteminį komponentą, arba aktyvuojama tik vidinėmis sąlygomis (pvz., prijungus per gamintojo konfigūravimo įrankį). Toks rezultatas rodo didesnį saugumo dėmesį – vengiant atvirų CGI įėjimų, sumažinamas atakų paviršius.

3.6. Programinės įrangos naujinių analizė

Atlikta išplėstinė kameros programinės įrangos *(angl. firmware)* analizė, siekiant nustatyti galimus tekstinius nutekėjimus ar įrašytas reikšmes, kurios galėtų būti išnaudotos atakoms. Panaudota išplėstinė analizė, skirta ieškoti reikšmių, susijusių su slaptažodžiais, vartotojais, shell komandomis, CGI nuorodomis `'user|pass|root|shell|port|cgi'`. Rezultatai parodė keletą nuorodų į galimas CGI funkcijas, tačiau nerasta konkrečių slaptažodžių ar galiojančių vartotojų vardų. Tai rodo, kad programinė įranga naudoja tinkamas saugumo praktikas – nesaugo jautrios informacijos atviru tekstu, o galimos funkcijos yra neaktyvios ar saugomos kituose segmentuose.

Atlikus nuoseklią ir daugiapakopę GeoVision IP kamerų analizę, nustatyta keletas reikšmingų įžvalgų. Kamera GV-EBD4813 yra potencialiai pažeidžiama „Slowloris“ tipo atakai, kas gali sutrikdyti jos veikimą per DoS mechanizmą. Tačiau kiti pažeidžiamumai, ypač susiję su RCE ar privilegijų eskalacija, nenustatyti. ONVIF sąsaja veikia korektiškai, tačiau reikalauja autentifikacijos ir naudoja tik POST metodą. 85 prievadas išlieka neidentifikuotas ir gali kelti riziką, ypač jei ten veikia paslėpta arba neapsaugota paslauga. Web sąsaja neatskleidžia visų aktyvių prievadų, o tai apsunkina administratoriaus galimybes kontroliuoti srautą. Firmware analizė parodė nedidelį tekstinės informacijos nutekėjimą, kas rodo teigiamą saugumo lygį. Bendra išvada – kamera yra sukonfigūruota pakankamai saugiai, tačiau kai kurie aspektai (pvz., 85 prievado paskirtis) turėtų būti toliau analizuojami ir stebimi siekiant užtikrinti visapusišką apsaugą.

Tačiau GeoVision GV-TBL4810 IP kamera šiuo metu turi vidutinio lygmens saugumo spragą dėl neužtikrintos HTTP sąsajos, leidžiančios neautentifikuotą prieigą prie konfigūracijos ir administravimo. Nors RTSP paslauga yra apsaugota, o CVE spragų tiesioginis išnaudojimas nepatvirtintas, įrenginys išlieka didelės rizikos dėl HTTP spragos ir nežinomos programinės įrangos versijos. Neatidėliotini pataisymo veiksmai – gamyklinis atstatymas, ugniasienės sugriežtinimas ir programinės įrangos atnaujinimas – yra būtini įrenginio apsaugai. Ilgalaikė apsauga priklausys nuo nuolatinio stebėjimo, tinklo segmentacijos ir atnaujintos programinės įrangos naudojimo.

Rekomendacijos ir skubūs veiksmai pastebėjus netinkamą konfiguraciją arba seną GeoVision kameros programinę įranga:

1. Autentifikacijos privalomas įjungimas HTTP sąsajose;
2. Prieigos ribojimas prie jautrių mazgų, pvz., */config.xml* tik tam tikriems IP adresams (pvz., 192.168.1.122);
3. Ugniasienės taisyklės HTTP srautui:
    a. iptables -A INPUT -p tcp -s 192.168.1.122 --dport 80 -j ACCEPT
    b. iptables -A INPUT -p tcp --dport 80 -j DROP
4. RTSP paslaugos išjungimas, jei nenaudojama:
    a. iptables -A INPUT -p tcp --dport 554 -j DROP
5. Programinės įrangos atnaujinimas per oficialią GeoVision svetainę. Jei įrenginys nebeturi palaikymo, svarstyti pakeitimą naujesniu modeliu;
6. Kameros atskyrimas VLAN tinkle, tokiu būtų sumažinama pažeidos rizika;
7. Įvykio žurnalų fiksavimas ir stebėjimas naudojant SIEM sistemas.

4. “ACTi Corporation” kamerų dinaminė analizė

Šioje dalyje pateikiama išsami dinaminė techninio saugumo analizė IP “ACTi Corporation” kameroms. Atliekant tyrimą, naudotas daugiasluoksnis įsilaužimo testavimo metodas, skirtas įvertinti visą kamerų pažeidžiamumo paviršių. Tai apima tinklo paslaugas, programinę įrangą, žiniatinklio sąsajas ir vaizdo transliavimo protokolus. Tyrimas vyko keliais etapais: tinklo žemėlapio sudarymas, API testavimas, protokolų pažeidžiamumo išnaudojimas, programinės įrangos analizė ir galinių taškų saugumo testavimas. Šie metodai leidžia simuliuoti realias atakas – nuo pasyvaus stebėjimo iki aktyvaus įsilaužimo – siekiant nustatyti visus galimus įėjimo taškus. Tyrimo rezultatai atskleidė svarbias rizikas: pasenusią programinę įrangą ir nežinomas paslaugas, kurios galėtų būti išnaudotos atakoms, pavyzdžiui, gauti prieigą prie tiesioginių vaizdo transliacijų arba naudoti kamerą kaip atspirties tašką tolimesnėms atakoms prieš tinklą.

Šios išvados skirtos informuoti suinteresuotąsias šalis apie kameros saugumo spragas ir pateikti praktines rekomendacijas jų šalinimui. Tai padės apsaugoti įrenginį nuo neteisėtos prieigos, duomenų nutekėjimo ir piktnaudžiavimo platesniame tinkle.

4.1. Tyrimo metodologija

Tyrimas atliktas remiantis „white-box“ testavimo metodika –analizė turėjo visą prieigą prie įrenginio vidaus, įskaitant konfigūracijos sąsajas ir tinklo aplinką. Tai leido giliau analizuoti kameros saugumo savybes ir aptikti subtilias konfigūracijos klaidas ar paslėptas spragas, kurios galėjo likti nepastebėtos taikant „black-box“ metodą. Visi bandymai buvo vykdomi kontroliuojamoje laboratorinėje aplinkoje, siekiant išvengti poveikio veikiančioms sistemoms ir užtikrinti etišką testavimą. “ACTi Corporation” kamerų tyrimo etapai:

1. Žvalgyba, atliekami pilno prievado skenavimai, paslaugų identifikavimas. Tikslas – suprasti, kurie tinklo taškai gali būti pažeidžiami;
2. Pažeidžiamumų paieška, įrenginio programinė įranga, API ir žiniatinklio sąsajos tiriamos dėl žinomų ar galimų saugumo spragų;
3. Išnaudojimo testavimas, tikrinama, ar aptiktos spragos gali būti išnaudotos praktiškai;
4. Saugumo stiprinimas, paruošiamos rekomendacijos ir scenarijai saugumui didinti;
5. Pakartotinis testavimas, tikrinamas taikytų apsaugos priemonių veiksmingumas ir ar jos nesukėlė naujų problemų.

4.2. Prievadų skenavimas ir įrenginio matomumo analizė

Atliktas išsamus IP kamerų prievadų skenavimas bei įrenginio sistemos identifikavimo bandymas naudojant prievadų analizės metodus. Šio proceso tikslas buvo nustatyti, kokios tinklo paslaugos aktyvios įrenginyje, kaip kamera save pateikia tinklo aplinkoje ir ar yra atvirų prievadų, kurie gali reikšti galimus saugumo pažeidimus ar nenumatytas prieigas. Pradinis skenavimas atliktas nustatyti ne tik atvirus TCP prievadus, bet ir identifikuoti veikiančias paslaugas bei operacinės sistemos tipą. Gauti rezultatai atskleidė atvirus šiuos prievadus:

1. 80/tcp: HTTP;
2. 6001/tcp & 6002/tcp, nežinomos, galimai vidinės binarinės paslaugos;
3. 7070/tcp, RTSP vaizdo transliavimas;
4. 20189/tcp, neįprastas HTTP atsakas, galimai klaidingai sukonfigūruota paslauga

Kameros paviršius atakai platesnis nei įprastai, įskaitant neaiškias paslaugas (6001, 6002, 20189), kurios gali būti nesaugios ar neapsaugotos.

4.3. Programinės įrangos naujinių analizė

Tyrimo metu buvo atliekama programinės įrangos naujinio specifinių instrukcijų paieška kuomet buvo ieškoma kameros išskleistoje programinėje įrangoje nuorodų į plačiai naudojamas kriptografines ar kitas bibliotekas. Buvo dekompiliuotas kodas į įskaitomą tekstą iš dvejetainių failų, kur filtruoti funkcijų ir bibliotekų pavadinimai, patikrai dėl standartinių šifravimo galimybių buvimo. Šis auditas buvo atliktas siekiant įvertinti, ar kamera palaiko saugius ryšio protokolus, nes stipraus kriptografijos nebuvimas galėtų sukelti pažeidžiamumus, tokius kaip nešifruotas duomenų perdavimas. Tyrimo metu nebuvo gauta jokia išvestis, kuri rodytų, kad „OpenSSL“ ar panašios kriptografinės bibliotekos nėra programinėje įrangoje. „OpenSSL“ nebuvimas rodo, kad kamera gali remtis silpnais arba patentuotais kriptografiniais metodais, jei jų išvis yra. Tai padidina nešifruoto ryšio, slaptažodžių saugojimo paprastu tekstu ir jautrumo atakoms, tokioms kaip „man-in-the-middle“ (MITM), riziką. Be standartinių šifravimo bibliotekų įrenginys gali perduoti jautrius duomenis, tokius kaip prisijungimo duomenys ar vaizdo srautai, paprastu tekstu, todėl užpuolikams lengva juos perimti ir išnaudoti. Šis atradimas pabrėžia būtinybę atnaujinti programinę įrangą arba pakeisti įrenginį modeliu, kuris palaiko modernius kriptografinius standartus. Žemiau paieškos pavyzdys specifinėms bibiliotekoms filtruoti:

```
strings decompressed.bin | grep -i openssl
```

Nerasta jokių užuominų apie OpenSSL. Tai rodo, kad kamera galimai neturi šiuolaikinių šifravimo funkcijų.

4.4. RTSP protokolo ir ONVIF sąsajos analizė

Šis tyrimas naudojo ffplay (FFmpeg dalis), siekiant bandyti pasiekti kameros RTSP vaizdo srautą be prisijungimo duomenų. RTSP dažnai naudojamas vaizdo srautiniam perdavimui IP kamerose, o neautentifikuota prieiga galėtų leisti bet kam tinkle peržiūrėti srautą, keldama didelę privatumo riziką. Nustatyta, kad sukonfigūravus komera naudoti slaptažodį srautas buvo pasiekiamas su autentifikacija. Tačiau kamera numatytuose nustatymuose nenaudoja autentifikacijos. Neautentifikuota RTSP prieiga yra kritinis pažeidžiamumas, nes ji leidžia bet kuriam vietinio tinklo vartotojui peržiūrėti kameros tiesioginį srautą be prisijungimo duomenų. Tai reiškia rimtą privatumo pažeidimą, nes neautorizuoti asmenys galėtų stebėti jautrias vietas, tokias kaip privati nuosavybė ar saugios patalpos. Platesnėje tinklo atakoje šis srautas galėtų būti

naudojamas žvalgybai ar informacijos rinkimui tolesniam išnaudojimui. Žemiau pateikiami bandymai naudojant RTSP srautus:

```
ffplay rtsp://192.168.1.107:7070
```

Šio bandymo metu buvo patikrinta ar srautas buvo pasiekiamas RTSP protokolu, naudojant įprastą medijos grotuvą. Taip pat buvo patikrinti siunčiami paketai juos surenkant naudojant *tshark* programį paketą. Duomenų rinkimui buvo naudojamas RTSP srautas per prievadą 7070, tikrinant šifravimo ir autentifikacijos antraštes. Kuomet autentifikacija yra nenaudojama šifravimo trūkumas dar labiau patvirtino srauto atvirumą.

Taip pat buvo atlikta ONVIF patikra kuomet tam tikslui buvo sukomponuotas programinis kodas:

```
from onvif import ONVIFCamera
cam = ONVIFCamera('192.168.1.107', 80, 'admin', admin0, '/etc/onvif/wsdl/')
media = cam.create_media_service()
try:
    stream_uri    =    media.GetStreamUri({'StreamSetup':    {'Stream':    'RTP-Unicast',
'Transport': 'UDP'}, 'ProfileToken': 'Profile_1'})
    print(f"Srauto URI: {stream_uri}")
except Exception as e:
    print(f"ONVIF Klaida: {e}")
```

Ši Python programa naudojo ONVIF protokolą, kad sąveikautų su kameros medijos paslaugomis, bandydamas gauti srauto URI. Programa tikrino, ar ONVIF reikalauja autentifikacijos, kas galėtų parodyti, ar kitos paslaugos yra panašiai neapsaugotos.

Nesukonfigūravus atitinkamai, įprastas RTSP srauto pasiekimas išryškina pagrindinį kameros prieigos kontrolės mechanizmų trūkumą. Šis pažeidžiamumas galėtų būti išnaudotas užpuolikų, norinčių stebėti kameros srautą, galimai sukeliant privatumo pažeidimus ar padedant fizinio saugumo atakoms.

4.5. API galinio taško analizė

API testavimas apima įvairių įvesčių siuntimą į galinį tašką, siekiant išbandyti jo tvarkymą su netikėtais ar kenksmingais duomenimis. Ši technika buvo naudojama nustatyti silpnybes, tokias kaip komandų įterpimas, parametrų tarša ir buferio perpildymai, kurie galėtų leisti užpuolikams manipuliuoti kameros konfigūracija ar vykdyti savavališką kodą. Pavyzdžiui, užpuolikas galėtų

įterpti kenksmingus parametrus, kad pakeistų nustatymus, gautų neautorizuotą prieigą ar sugadintų paslaugą. Atlikti testavimui buvo sukomponuotas programinis kodas:

```
import requests, string, random
url = "http://192.168.1.107/api/v1/config"
payloads = [''.join(random.choices(string.printable, k=10)) for _ in range(20)]
methods = ["GET", "POST", "PUT"]

for method in methods:
        for payload in payloads:
                try:
                    response = requests.request(method, url, data={'param': payload}, timeout=5)
                    if response.status_code != 400 and response.status_code != 404:
                        print(f"Metodas:      {method},      Krovinys:      {payload},      Būsena:
{response.status_code}, Atsakymas: {response.text[:50]}")
                except requests.RequestException as e:
                    print(f"Klaida: {e}")
```

Testavimo kodas išbandė */api/v1/config* galinį tašką su atsitiktiniais simboliais per GET, POST ir PUT metodus, siekiant nustatyti netikėtą elgseną. Klaidų atsakymai parodė, kad galinis taškas nėra pažeidžiamas tolesniam išnaudojimui, tokiam kaip komandų įterpimas ar privilegijų eskalacija. Hipotezė, kad galinis taškas buvo išjungtas, ribojamas ar filtruojamas po aptikimo, rodo, kad kamera gali turėti pagrindines įsibrovimų aptikimo galimybes, tačiau jos yra nepakankamos visiškai apsaugoti galinį tašką.

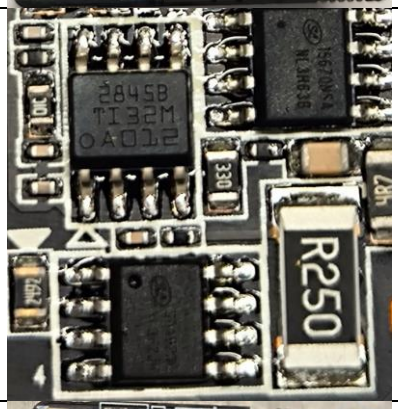
5. Aparatinė gaminių analizė

Nustatyta, kad gaminiuose įgyvendinti tipiniai elektroninių mazgų sprendimai, realizacija atlikta ekonominėje gamybos bazėje 2, 4, 6, 8 lentelėse pateikiami „ACTi Corporation“ ir „GeoVision“ kamerų elektronikos elementus gaminančių įmonių pavadinimai ir jų pagrindinės įsikūrimo vietovės. Galima teigti, kad įrenginiuose veikianti programinė įranga yra pritaikyta funkcionuoti konkrečių lustų rinkinių bazėje. 1, 3, 5, 7 lentelėse pateikiami „ACTi Corporation“ ir „GeoVision“ kamerų elektronikos dekompozicijos tyrimų rezultatai.

Lentelė 1. „ACTi Corporation A423” kameros elektronikos dekompozicijos tyrimo rezultatai.

“ACTi Corporation” kameros A423-00AXX-24A-0259 aparatinės dalie apžvalga		
		Ethernet ryšio linija plokštę pasiekia ne vytos poros tipo laidais. Dėl šios priežasties gali kilti komunikacijos su kamera problemų.
		Pateikiamas kameros viršaus vaizdas, be korpuso. Kamera susideda iš maitinimo, pagrindinės ir sensoriaus plokščių. Naudojama impulsinė maitinimo grandinės realizacija reikiamoms įtampoms išgauti.
		Pagrindinės plokštės vaizdas iš viršaus. Matomas DDR3(L) 4Gb SDRAM laikinosios atminties lustas viršuje dešiniajame kampe, pagrindinės komunikacinės jungtys, kurios priima signalus iš kameros sensoriaus, išorinių periferijų signalus, maitinimo linijas. Matomas 1 RESET mygtukas, kuris yra prieinami neišardžius kameros, atidarius apsauginį dangtelį.

		Pateikiamas pagrindinės plokštės apatinės pusės vaizdas. Kairėje pusėje po dangteliu matosi paslėpti aukštos integracijos SoC (System-on-Chip) ARM procesorius ir 256 Mb DDR SDRAM atminties mikroschema. Šios plokštės viršuje, taip pat yra matomas SD kortelės lizdas, žemiau dešinėje pusėje objektyvo sistemos variklių valdymo lustas ir apačioje kairėje pusėje FLASH atminties lustas.
		Kaip pagrindinis procesorius vaizdo signalų apdorojimui yra naudojamas „Novatek Microelectronics Corp“ gamintojo „NT98529BG“ mikrovaldiklis. Tai aukštos integracijos SoC (System-on-Chip) ARM procesorius.
		Kaip pagrindinė atmintis naudojama „NT5C8256M16ER-FL“, kurį gamina „Nanya Technology Corporation“. Tai 256 Mb DDR SDRAM (Double Data Rate Synchronous DRAM) atminties mikroschema.
		Taip pat yra naudojamas to paties gamintojo „Nanya Technology Corporation“ „NT5CB256M16ER-FL“ DDR3(L) 4Gb SDRAM laikinosios atminties lustas.
		Kameros objektyvo sistemos variklių valdymui naudojamas „MediaTek“ gamintojo „MS35009“ mikrovaldiklis. Komunikacijai su varikliais naudojama SPI sąsają.

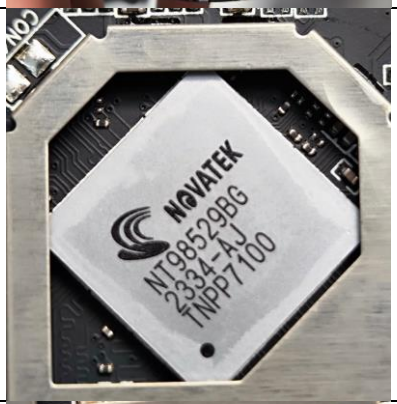
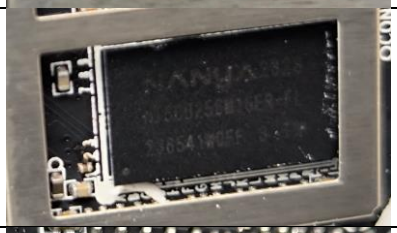
		„Winbond Electronics Corporation“ gamintojo NAND FLASH 1Gbit (128MB) „W25N01GVZEIG“ atminties lustas. Šis lustas gali būti naudojamas duomenims saugoti arba kitiems nepastoviems duomenims registruoti, kurie reikalingi įterptinėse sistemose. Turi 1 Gbit talpą ir palaiko SPI / Dual SPI / Quad SPI sąsajas.
		Maitinimo plokštės vaizdas iš viršaus. Matomos pagrindinės maitinimo jungtys ir įtampos reguliavimo komponentai.
		Maitinimo plokštės vaizdas iš apačios. Matomi dešinėje apačioje esantys įtampos valdiklis, MOSFET tranzistorius ir maitinimo įrenginio (PD) valdiklis.
		Kameroje naudojama „Texas Instrument“ gamintojo „TL2845B” DC/DC įtampos valdiklis ir “Silan microelectronics” gamintojo “SVG15670NSA 1A”, 150V N-CHANEL MOSFET tranzistorius ir “SD4923E“ MOSFET PoE maitinimo įrenginio (PD) valdiklis suderinamas su IEEE 802.3AF/AT standartu.
		Pateikiamas sensoriaus plokštės apatinės pusės vaizdas.

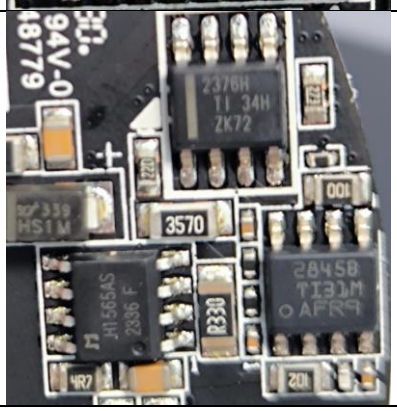
Lentelė 2. „ACTi Corporation A423" kameros pagrindinių elektronikos komponentų gamintojų adresai.

Įmonės pavadinimas	**Įmonės pagrindinis adresas**
„Nanya Technology Corporation"	Nanlin Rd., Taishan Dist, New Taipei City 243, Taiwan (R.O.C.)
„MediaTek"	Dusing 1st Rd., Hsinchu Science Park, Hsinchu City 300, Taiwan
„Winbond"	Keya 1st Rd., Daya Dist., Central Taiwan Science Park, Taichung City 428303, Taiwan
„Texas Instrument"	Dallas, Texas 75243 USA
"Silan microelectronics"	HuangGuShan Road, HangZhou, China
„Novatek Microelectronics Corp"	Innovation Road II, Hsinchu Science Park, Hsinchu 300, Taiwan

Lentelė 3. „ACTi Corporation A77” kameros elektronikos dekompozicijos tyrimo rezultatai.

“ACTi Corporation A77” kameros A77-00AXXX-24E-0497 aparatinės dalie apžvalga	
	Kameros vaizdas nuėmus viršutinę korpuso dalį. Matoma pagrindinė plokštė ir impulsinio maitinimo komponentai.
	Kameros vaizdas nuėmus pagrindinę plokštę. Ethernet ryšio linija plokštę pasiekia ne vytos poros tipo laidais. Dėl šios priežasties gali kilti komunikacijos su kamera problemų.
	Pagrindinės plokštės vaizdas iš viršaus. Matomos visos komunikacinės jungtys, kurios priima signalus iš kameros sensoriaus, išorinių periferijų, maitinimo linijas. Taip pat yra matomas 1 valdymo mygtukas, kuris yra prieinami tik išardžius kameros apsaugines dalis, SD kortelės lizdas viršuje dešiniajame kampe, DDR3(L) 4Gb SDRAM laikinosios atminties lustas, „FLASH“ atminties lustas.

		Pateikiamas pagrindinės plokštės apatinės pusės vaizdas. Viršuje po dangteliu matosi paslėpti aukštos integracijos SoC (System-on-Chip) ARM procesorius ir 256 Mb DDR SDRAM atminties mikroschema. Taip pat apačioje yra matomi aukštos galios (PD) valdiklis ir DC/DC įtampos valdiklis.
		Kaip pagrindinis procesorius vaizdo signalų apdorojimui yra naudojamas „Novatek Microelectronics Corp“ gamintojo „NT98529BG“ mikrovaldiklis. Tai aukštos integracijos SoC (System-on-Chip) ARM procesorius.
		Kaip pagrindinė atmintis naudojama „NT5C8256M16ER-FL“, kurį gamina „Nanya Technology Corporation“. Tai 256 Mb DDR SDRAM (Double Data Rate Synchronous DRAM) atminties mikroschema.
		Taip pat yra naudojamas to paties gamintojo „Nanya Technology Corporation“ „NT5CB256M16ER-FL“ DDR3(L) 4Gb SDRAM laikinosios atminties lustas.
		„Winbond Electronics Corporation“ gamintojo NAND FLASH 1Gbit (128MB) „W25N01GVZEIG“ atminties lustas. Šis lustas gali būti naudojamas duomenims saugoti arba kitiems nepastoviems duomenims registruoti, kurie reikalingi įterptinėse sistemose. Turi 1 Gbit talpą ir palaiko SPI / Dual SPI / Quad SPI sąsajas.

		"Maxim Technology (FPE)" gamintojo „LX16106SN“ ethernet tinklo transformatorių modulis, kuris tinka 10/100 Mbps Ethernet ryšiui.
		Kameroje naudojama „Texas Instrument“ gamintojo „TPS2376-H“ PoE PD (Powered Device) valdiklis suderinamas su IEEE 802.3af standartu ir „TL2845B” DC/DC įtampos valdiklis. Taip pat matomas „Jiangsu Jiejie Microelectronics“ gamintojo „JMSH1565AGS/ JMSH1565APS“ N-tipo MOSFET valdiklis.

Lentelė 4. „ACTi Corporation A77” kameros pagrindinių elektronikos komponentų gamintojų adresai.

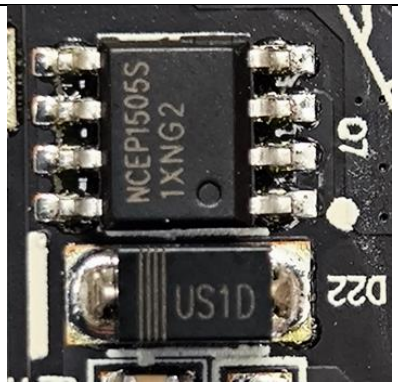
Įmonės pavadinimas	Įmonės pagrindinis adresas
„Novatek Microelectronics Corp“	Innovation Road II, Hsinchu Science Park, Hsinchu 300, Taiwan
„Nanya Technology Corporation“	Nanlin Rd., Taishan Dist, New Taipei City 243, Taiwan (R.O.C.)
„Winbond“	Keya 1st Rd., Daya Dist., Central Taiwan Science Park, Taichung City 428303, Taiwan
"Maxim Technology (FPE)"	Xinnan Jinhu 1st Road, Qishi Town, Dongguan City, China.
„Texas Instrument“	Dallas, Texas 75243 USA.
„Jiangsu Jiejie Microelectronics“	Qiantangjiang Road, Economic Development Zone, Qidong City, Jiangsu Province, China.

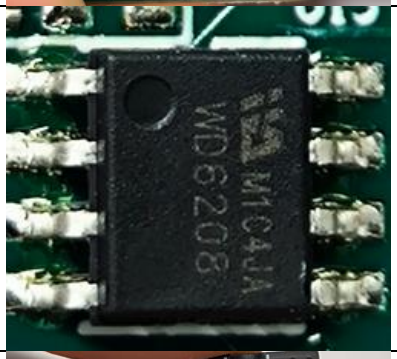
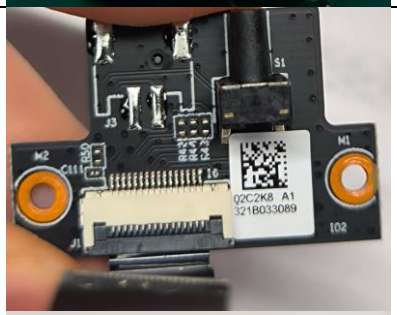
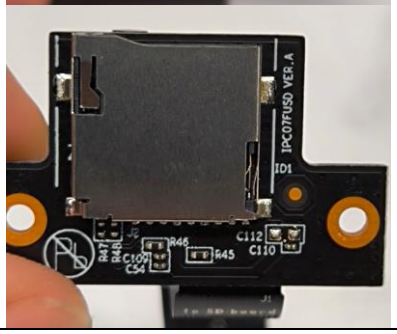
Lentelė 5. „GeoVision Inc GV-EBD4813” kameros elektronikos dekompozicijos tyrimo rezultatai.

„GeoVision Inc GV-EBD4813” kameros 210235TRBH321C010230 aparatinės dalie apžvalga

		Ethernet ryšio linija plokštę pasiekia ne vytos poros tipo laidais. Dėl šios priežasties gali kilti komunikacijos su kamera problemų.
		Pateikiamas išardytos kameros vaizdas iš viršaus, be korpuso. Kamera susideda iš pagrindinės, sensoriaus ir duomenų/signalų perdavimo plokščių. Naudojama impulsinė maitinimo grandinės realizacija reikiamoms įtampoms išgauti.
		agrindinės plokštės vaizdas iš viršaus. Matomas pagrindinis duomenų apdorojimo lustas centre, dalis komunikacinių jungčių, kurios priima/atiduoda signalus į pagrindinį valdiklį ir užmaitina pačią kamerą, perduoda duomenis į išorinę atmintį. Šioje plokštėje matomas „SSC30KQ“ pagrindinis mikrovaldiklis, NAND FLASH 1Gbit (128MB) „MX35LF1GE4AB“ atminties lustas ir objektyvo valdymo „MS41929“ mikrovaldiklis ir apsauginis MOSFET (tranzistorius) „BT16B03“.

		Pateikiamas pagrindinės plokštės vaizdas iš apačios. Šioje pusėje yra matomas „TPS23753A“ maitinimo ir duomenų perdavimą per Ethernet kabelį (PoE) valdiklis, N-tipo „NCEP1505S“ MOSFET tranzistorius, bei kita dalis komunikacinių jungčių, kurios priima/atiduoda signalus iš kameros sensoriaus, kameros variklių valdymo.
		Pagrindinis SSC30KQ „SigmaStar Technology“ gamintojo, ARM architektūros mikrovaldiklis yra naudojamas vaizdų, tinklo ryšių, bendrų sistemos duomenų apdorojimui ir valdymui.
		„Macronix international“ gamintojo NAND FLASH 1Gbit (128MB) „MX35LF1GE4AB“ atminties lustas. Šis lustas gali būti naudojamas duomenims saugoti arba kitiems nepastoviems duomenims registruoti, kurie reikalingi įterptinėse sistemose.
		Kameros objektyvo sistemos variklių valdymui naudojamas „Ruimeng Technology“ gamintojo „MS41929“ mikrovaldiklis. Komunikacijai naudoja SPI sąsają.

		Kameroje naudojamas „NCEPOWER“ gamintojo „NCEP1505S“ N-tipo MOSFET tranzistorius.
		Texas Instrument“ gamintojo „TPS23753A“ valdiklis, kuris skirtas „Power over Ethernet“ (PoE) maitinamų įrenginių (PD) sąsajai ir izoliuoto tipo DC-DC keitiklio valdymui. Jis atitinka IEEE 802.3at standartą ir palaiko iki 13W galios tiekimą per Ethernet tinklą.
		Pateikiamas optinio sensoriaus plokštės vaizdas iš apačios ir viršaus. Šios plokštės apačioje yra matomas variklių valdymo „WD6208“ lustas.

		
		Kameroje naudojamas „Wade Semiconductor“ gamintojo WD6208 variklių valdymo lustas.
	 	Pateikiamas GSM ryšio (SIM lizdo) ir RESET mygtukui išskirtos plokštės vaizdas iš viršaus ir apačios. Vienoje pusėje yra matomas RESET valdymo mygtukas, kuris yra prieinami tik išardžius kameros apsaugines dalis ir valdymo jungtis, jungianti su pagrindiniu procesoriumi.. Taip pat, kitoje pusėje yra matomas SD kortelės lizdas.

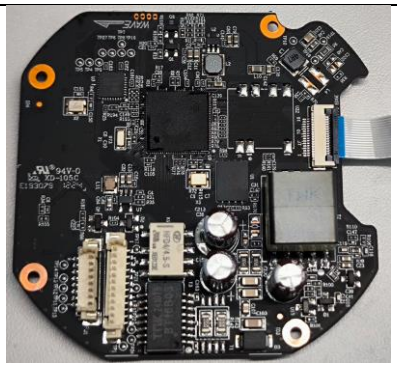
Lentelė 6. „GeoVision Inc GV-EBD4813” kameros pagrindinių elektronikos komponentų gamintojų adresai.

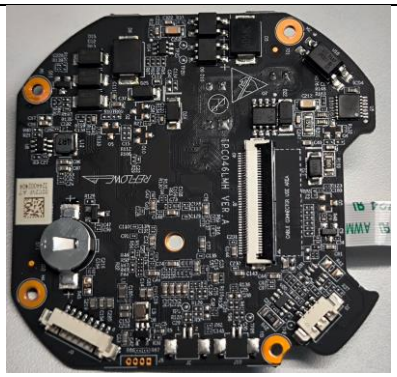
Įmonės pavadinimas	Įmonės pagrindinis adresas
„SigmaStar Technology“	Houzhan Road, Tongan District, Xiamen, China
„Macronix international“	Li-Hsin Road, Science Park, Hsinchu, Taiwan

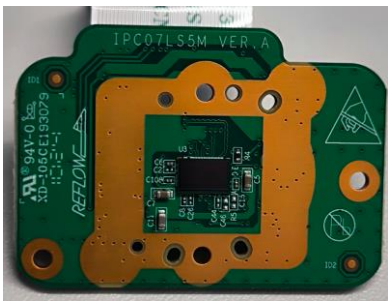
„Ruimeng Technology“	Weiye Road, Binjiang District, Hangzhou, China
„NCEPOWER“	East of Kyanji 1st Road, Xinwu District, Wuxi City, China
„Texas Instrument“	Dallas, Texas 75243 USA.
„Wade Semiconductor“	Junxiang U8 Intelligent Manufacturing Industrial Park, Hangcheng Avenue, Gushu Community, Xixiang Street, Bao'an District, Shenzhen, Guangdong, China

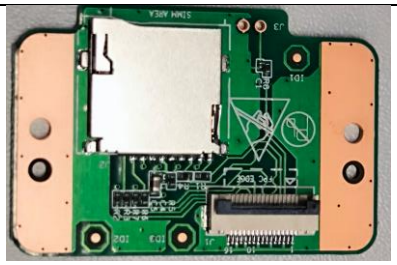
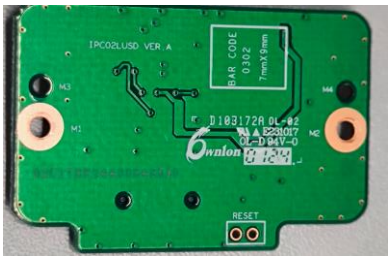
Lentelė 7. „GeoVision Inc GV-TBL4810” kameros elektronikos dekompozicijos tyrimo rezultatai.

„GeoVision Inc GV-TBL4810” kameros 210235TRBF3244002383 aparatinės dalie apžvalga	
	Ethernet ryšio linija plokštę pasiekia ne vytos poros tipo laidais. Dėl šios priežasties gali kilti komunikacijos su kamera problemų.

	Pateikiamas išardytos kameros vaizdas iš viršaus, be korpuso. Kamera susideda iš pagrindinės, sensoriaus ir duomenų/signalų perdavimo plokščių. Naudojama impulsinė maitinimo grandinės realizacija reikiamoms įtampoms išgauti.
	Pagrindinės plokštės vaizdas iš viršaus. Matomas pagrindinis duomenų apdorojimo lustas, kurio centre pagrindiniai valdikliai, taip pat matoma dalis komunikacinių jungčių, kurios priima/atiduoda signalus į pagrindinį valdiklį ir užmaitina pačią kamerą, perduoda duomenis į išorinę atmintį. Šioje plokštėje yra „SSC30KQ“ pagrindinis mikrovaldiklis, NAND FLASH 1Gbit (128MB) „W25N01GVZEIG“ atminties lustas, objektyvo valdymo „MS41929“ mikrovaldiklis, „HFD4/4.5-S“ rėlė ir apsauginis MOSFET (tranzistorius) „BT16B03“.

	Pateikiamas pagrindinės plokštės apatinės pusės vaizdas. Šioje pusėje yra matomas „TPS23753A“ maitinimo ir duomenų perdavimą per Ethernet kabelį (PoE) valdiklis, N-tipo „SM01F03“ MOSFET tranzistorius, bei kita dalis komunikacinių jungčių, kurios priima/atiduoda signalus iš kameros sensoriaus, kameros variklių valdymo.
	Pagrindinis SSC30KQ „SigmaStar Technology“ gamintojo, ARM architektūros mikrovaldiklis yra naudojamas vaizdų, tinklo ryšių, bendrų sistemos duomenų apdorojimui ir valdymui.
	„Winbond Electronics Corporation“ gamintojo NAND FLASH 1Gbit (128MB) „W25N01GVZEIG“ atminties lustas. Šis lustas gali būti naudojamas duomenims saugoti arba kitiems nepastoviems duomenims registruoti, kurie reikalingi įterptinėse sistemose. Turi 1 Gbit talpą ir palaiko SPI / Dual SPI / Quad SPI sąsajas.
	Kameros objektyvo sistemos variklių valdymui naudojamas „Ruimeng Technology“ gamintojo „MS41929“ mikrovaldiklis. Komunikacijai naudoja SPI sąsają.

	Kameroje taip pat naudojama „Hongfa Technology“ gamintojo „HFD4/4.5-S“ signalinė rėlė ir „Dongguan Xinkang Electronic Technology“ gamintojo „BT16B03“ apsauginis MOSFET (tranzistorius) užtikrinantis signalų izoliaciją ir atitinka IEEE 802.3u standartą.
	„Texas Instrument“ gamintojo „TPS23753A“ valdiklis, kuris skirtas „Power over Ethernet“ (PoE) maitinamų įrenginių (PD) sąsajai ir izoliuoto tipo DC-DC keitiklio valdymui. Jis atitinka IEEE 802.3at standartą ir palaiko iki 13W galios tiekimą per Ethernet tinklą.
 	Pateikiamas optinio sensoriaus plokštės vaizdas iš apačios ir viršaus. Šios plokštės apačioje yra matomas variklių valdymo „WD6208“ lustas.

	Kameroje naudojamas „Wade Semiconductor“ gamintojo „WD6208“ variklių valdymo lustas.
 	Pateikiamas GSM ryšio (SIM lizdo) ir RESET mygtukui išskirtos plokštės vaizdas iš viršaus ir apačios. Vienoje pusėje yra matomas RESET valdymo mygtukui išskirti kontaktai, kurie yra prieinami tik išardžius kameros apsaugines dalis. Taip pat, kitoje pusėje yra matomas SD kortelės lizdas ir valdymo jungtis, jungianti su pagrindiniu procesoriumi.

Lentelė 8. „GeoVision Inc GV-TBL4810” kameros pagrindinių elektronikos komponentų gamintojų įmonės ir jų adresai.

Įmonės pavadinimas	Įmonės pagrindinis adresas
„SigmaStar Technology“	Houzhan Road, Tong'an District, Xiamen City, Fujian Province, 361116, China
„Winbond Electronics Corporation“	Keya 1st Rd., Daya District, Central Taiwan Science Park, Taichung City 428303, Taiwan.
„Ruimeng Technology“	Weiye Road, Binjiang District, Hangzhou, China.
„Hongfa Technology“	Donglin Road, North Jimei Industrial Zone, Xiamen, Fujian, 361021, China.
„Dongguan Xinkang Electronic Technology“	Xinshi 3rd Road, Xinshi Community, Chang’an Town, Dongguan City, Guangdong Province, China.
„Texas Instrument“	12500 TI Boulevard, Dallas, Texas 75243, USA.

„Wade Semiconductor“	Xingye Road, Nanshan District, Shenzhen, Guangdong Province, China

Šaltiniai

[1] ACTi darbuotojų skaičius. https://growjo.com/company/ACTi_Corporation?utm_source=chatgpt.com
[2] ACTi kompanijos profilis. https://www.acti.com/corporate/about#about
[3] Yahoo Finance. https://finance.yahoo.com/quote/5240.TWO/
[4] ACTi Q2 „Product Matrix“ katalogas. https://www.acti.com/products
[5] GeoVision darbuotojų skaičius https://pitchbook.com/profiles/company/169837-30?utm_source=chatgpt.com#overview
[6] GeoVision kompanijos profilis. https://www.geovision.com.tw/aboutCompany.php
[7] ACTi kompanijos bendradarbiavimas su Geovision įmone. https://www.acti.com/cloud/Geovision-acti
[8] ACTi kompanijos bendradarbiavimas su HIKVISION įmone. https://www.acti.com/cloud/hikvision-acti
[9] ACTi kompanijos bendradarbiavimas su Dahua įmone. https://www.acti.com/cloud/Dahua-acti
[10] ACTi kompanijos bendradarbiavimas su kitomis įmonėmis. https://www.acti.com/solutionpartners
[11] ACTi kompanijos. Kameros „A423-00AXX-24A-0259“ specifikacija. https://download.acti.com?id=31772
[12] ACTi kompanijos. Kameros „A77-00AXXX-24E-0497“ specifikacija. https://download.acti.com?id=31490
[13] GeoVision Inc“ kompanijos. Kameros „GV-TBL4810“ specifikacija. https://s3.amazonaws.com/geovision_downloads/Manual/IPCAM/Datasheet/TBL/Datasheet_IPCamTBL4810.pdf
[14] GeoVision Inc“ kompanijos. Kameros „GV-EBD4813“ specifikacija. https://s3.amazonaws.com/geovision_downloads/Manual/IPCAM/Datasheet/Eyeball/Datasheet_IPCamEBD4813.pdf