MPC-2610

Su sauga susijusios atsargumo priemonės

Šis žinynas apibūdina su sauga susijusias atsargumo priemones perduodant failus ir transliuojant iš įrenginio.

MPC-2610
Su sauga susijusios atsargumo priemonės

Su sauga susijusios atsargumo priemonės

Šioje temoje apibūdinamos atsargumo priemonės, kurių reikia paisyti prijungiant įrenginį prie tinklo.

- Komunikacijos turinį jums nežinant gali perimti neįgaliotosios trečiosios šalys, esančio netoli signalo. Naudodami belaidį LAN ryšį, įdiekite tinkamas saugumo priemones, kad apsaugotumėte komunikacijos turinį.
- Jei nustatote [Security] belaidžio LAN ryšio nuostatą kaip [None] ir jungiatės prie prieigos taško, belaidis ryšys tarp fotoaparato ir prieigos taško nebus šifruotas ir signalo diapazone jį gali perimti trečioji šalis. Siekdami didesnio saugumo naudokite WPA2 arba WPA3 saugumo protokolą.
- „SONY“ NEATSAKO UŽ BET KOKIO POBŪDŽIO NUOSTOLIUS, ATSIRADUSIUS DĖL PERDAVIMO ĮRENGINIUOSE NEĮDIEGTŲ SAUGOS PRIEMONIŲ, DĖL SU PERDAVIMO CHARAKTERISTIKOMIS SUSIDARIUSIO NEIŠVENGIAMO DUOMENŲ NUTEKĖJIMO ARBA BET KOKIO TIPO SAUGOS PROBLEMŲ.
- Atsižvelgiant į darbo aplinką, tinklu besinaudojančios ir neturinčios leidimo trečiosios šalys gali įgyti prieigą prie įrenginio. Jungdami įrenginį į tinklą būtinai įsitikinkite, kad tinklas tinkamai apsaugotas.
- Jungdami šį gaminį prie tinklo, junkite per sistemą, kuri užtikrina apsaugos funkciją, pvz., maršruto parinktuvą arba užkardą. Jungiant be tokios apsaugos, gali kilti saugumo problemų.

TP1002221081

MPC-2610
Su sauga susijusios atsargumo priemonės

Atsargumo priemonės, susijusios su interneto ryšiu

Šioje temoje apibūdinamos atsargumo priemonės, kurių reikia paisyti prijungiant įrenginį prie interneto.

- Įrenginys belaidžiu LAN ryšiu negali prisijungti prie prieigos taško, kuris naudoja tik WEP arba WPA, nes šie saugumo metodai yra pažeidžiami.
- Įrenginys nėra tinklo įrenginys (pavyzdžiui, maršruto parinktuvas arba šakotuvas). Primygtinai rekomenduojama įrenginį jungti prie tinklo, kuriame galite tinkamai konfigūruoti ir valdyti tinklo nuostatas, kad apsisaugotumėte nuo prieš tinklą nukreiptų atakų, pvz., DoS atakos (aptarnavimo perkrovos atakos).
- Prijungdami įrenginį prie tinklo junkite jį per maršruto parinktuvą, kuris tinkamai sukonfigūruotas ir valdomas, arba junkite prie LAN prievado, kurio funkcijos tokios pačios. Jei jungiate be tokios apsaugos (pavyzdžiui, naudodami nemokamą „Wi-Fi“), gali kilti saugumo problemų. Tinkamai sukonfigūruoti maršruto parinktuvai suteikia pakankamą apsaugą nuo DoS atakų arba įrenginių funkcionalumo praradimo tinkle. Jei pastebite ką nors nepaprasto, nedelsdami atjunkite fotoaparatą nuo tinklo.

TP1002221082

MPC-2610
Su sauga susijusios atsargumo priemonės

Atsargumo priemonės, susijusios su tinklo funkcija

Šioje temoje apibūdinamos atsargumo priemonės, susijusios su įrenginio tinklo funkcija.

- Jei aptinkama neleistina prieiga, fotoaparatas gali nebepriimti ryšio. Tokiu atveju iš naujo prijunkite nuo pradžios.
- Autentifikavimo informacija, reikalinga prisijungti prie įrenginio, rodoma, kai naudojate [Network] – [Network Setup] – [Show Authentication]. Pasirūpinkite, kad ekrano nematytų ir QR kodo vaizdo negalėtų nukopijuoti kiti asmenys.
- Naudotojo vardas ir slaptažodis turi būti nustatyti įsigijimo momentu. Kai nustatote savo naudotojo vardą ir slaptažodį, įsitikinkite, kad nuostatų nemato kiti asmenys. Nustatykite naudotojo vardą ir slaptažodį tokia tvarka.

[User Name]	– Naudotojo vardą turi sudaryti nuo 1 iki 16 ženklų. – Gamykloje vardas nustatytas į „admin“. – Toliau pateikiami galimi įvesti simboliai. Raidės (didžiosios ir mažosios), skaitmenys, simboliai (! % + , - . = _)
[Password]	– Nustatykite 8–16 simbolių ilgio slaptažodį, kuriame būtų bent 1 ar daugiau raidžių ir 1 ar daugiau skaitmenų. – Toliau pateikiami galimi įvesti simboliai. Raidės (didžiosios ir mažosios), skaitmenys, simboliai (! % + , - . = _)

TP1002221083

MPC-2610
Su sauga susijusios atsargumo priemonės

Atsargumo priemonės, susijusios su belaidžiu LAN

Šioje temoje apibūdinamos atsargumo priemonės, kurių reikia paisyti prijungiant įrenginį belaidžiu LAN ryšiu.

- Šio įrenginio žinyne belaidžio LAN prieigos taškai ir belaidžio LAN maršruto parinktuvai, kurie perduoda LAN ryšius, vadinami „prieigos taškais“.
- [Security] (šifravimo būdas) galima nustatyti kaip [None], [WPA2] arba [WPA3]. Saugumo požiūriu rekomenduojama nustatyti [WPA2] arba [WPA3]. Kai [None] pasirinkta, prieš prisijungiant rodomas pranešimas. Kad belaidis LAN ryšys būtų saugus, primygtinai rekomenduojama prie prieigos taškų jungtis naudojant WPA2 arba WPA3 saugos nuostatą.
- Pagal numatytąją nuostatą, pasirenkamas WPA2 saugos metodas, kai registruojamasi prie bevielio LAN tinklo prieigos taško naudojant [Manual Register].
- Jei prie prieigos taško jungiatės be jokios saugos nuostatos, galite nukentėti nuo įsilaužėlių, kenkėjiškų trečiųjų šalių prieigos ar atakų prieš pažeidžiamas vietas. Nerekomenduojama užmegzti ryšio be jokių saugos nuostatų, nebent tai neišvengiama.
- Sukonfigūruoti belaidžio LAN ryšio saugumą yra labai svarbu. „Sony“ neprisiima atsakomybės už jokią žalą, kilusią dėl to, kad nebuvo imtasi saugumo priemonių, arba jei saugumo problema naudojant belaidį LAN ryšį kilo dėl neišvengiamų aplinkybių.

TP1002221084

MPC-2610
Su sauga susijusios atsargumo priemonės

Atsargumo priemonės, susijusios su dalijimusi interneto ryšiu per USB

Šioje temoje apibūdinamos atsargumo priemonės, kurių reikia paisyti prijungiant įrenginį per USB.

- Internetu dalykitės tik su patikimais išmaniaisiais įrenginiais. Dėl saugumo nerekomenduojama prisijungti prie nežinomos kilmės įrenginių.

TP1002221085

MPC-2610
Su sauga susijusios atsargumo priemonės

Apie FTPES (FTPS) funkciją

FTPS funkcija palaiko įvairius šifravimo algoritmus, kad būtų užtikrintas saugus failų perdavimas. Įvairūs šifravimo algoritmai, iš kurių ne visi gali atitikti dabartinę geriausią saugumo praktiką, palaikomi dėl suderinamumo su įvairiais serveriais.

FTPS funkcijos palaikomi šifravimo algoritmai

Palaikomi toliau nurodyti šifravimo algoritmai.

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Rekomenduojami šifravimo algoritmai

Toliau nurodyti šifravimo algoritmai yra rekomenduojami pagal NIST rekomendacijas (NIST SP 800-57, 1 dalis, 5 redakcija) ir susijusius saugumo standartus.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Apie pasenusius algoritmus

FTPS funkcija taip pat palaiko toliau nurodytus algoritmus dėl suderinamumo, tačiau pagal NIST rekomendacijas (NIST SP 800-57, 1 dalis, 5 redakcija) ir susijusius saugumo standartus jie yra pasenę ir būsimose versijose gali būti pašalinti.

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

Apie ryšio suderinamumą

FTPS funkcija sukurta subalansuojant saugumą ir suderinamumą. Šiuo metu pasenę algoritmai palaikomi dėl toliau nurodytų priežasčių, bet būsimose versijose gali būti pašalinti siekiant didesnio saugumo.

- Laisvai samdomiems fotografams ir videografams reikia prisijungti prie įvairių klientų serverių.
- Turi būti išlaikytas suderinamumas su senesnėmis sistemomis ir senstelėjusiais serveriais.
- Ne visi naudotojai yra pasirengę pereiti prie saugesnių nustatymų, nes šifravimo algoritmų nuostatų keitimas serverio pusėje yra sudėtingas.
- FTPS nuostatos dažnai bendrinamos su kitomis saugumo paslaugomis. Bet kokius pakeitimus būtina gerai apgalvoti, nes jie gali turėti įtakos ir kitoms serverio paslaugoms.
- Turi būti palaikomi įvairūs šifravimo algoritmai, kad būtų užtikrinta sąveika skirtingose aplinkose.

Šifravimo algoritmai, naudojami per FTPS ryšį, nustatomi vedant automatines derybas su paskirties vietos serveriu, todėl priklauso nuo serverio nuostatų. Nors žinoma apie saugumo rizikas, šiuo metu pirmenybė teikiama suderinamumui, kad būtų tenkinami įvairūs naudotojų poreikiai.

Saugumo rizikos

Naudojant pasenusius algoritmus, įskaitant CBC / DHE / RSA / SHA-1, padidėja rizika, kad užšifruoti duomenys bus iššifruoti arba sugadinti įsibrovėlio ir atskleisti transliavimo metu.

Saugaus ryšio rekomendacijos

Prieš naudodami FTPS funkciją patikrinkite, ar ryšio paskirties vietos serveris palaiko rekomenduojamą šifravimo algoritmą. Serverio pusėje įgalinkite tik rekomenduojamus algoritmus ir išjunkite pasenusius algoritmus.

Įkeliama naudojant saugų FTP

Galite įkelti šifruotus failus naudodami FTPS, per atskirojo režimo (FTPES) ryšį su paskirties failų serveriu.
Norėdami saugiai perkelti per FTP, nustatykite [Using Secure Protocol] to [On] failų perdavimo paskirties serverio nustatymuose ir importuokite sertifikatą.

Nuorodos

- Recommendation for Key Management, Special Publication 800-57 Part 1 Revision 5, NIST, 2020.
- Transitioning the Use of Cryptographic Algorithms and Key Lengths, Special Publication 800-131A Revision 2, NIST, 2019.
- Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, NIST, 2005 (įskaitant atnaujinimus nuo 2016-10-06).

Sertifikatas

Įrašykite FTPES (FTPS) funkcijos naudojamą sertifikatą į atminties kortelės šakninį katalogą. Nustatykite pavadinimą, kaip nurodyta toliau.
certification.pem (PEM formatas)
Didžiausias sertifikatas, kurį galima įkelti, yra 1 MB vienam sertifikatui.

TP1002221086