SONY

Abijuhend

MPC-2610

Turvalisuse ettevaatusabinõud

See abijuhend kirjeldab seadmega faili- ja voogedastuse turvalisuse ettevaatusabinõusid.

MPC-2610
Turvalisuse ettevaatusabinõud

Turvalisuse ettevaatusabinõud

Selles teemas kirjeldatakse seadme võrguga ühendamise ettevaatusabinõusid.

- Signaalide läheduses asuvad volitamata muud osapooled võivad võrgusuhtluse sisu teile teadmata kinni püüda. Traadita kohtvõrgu sidet kasutades rakendage turvameetmed nõuetekohaselt, et kaitsta võrgusuhtluse sisu.
- Kui määrate traadita kohtvõrgu suvandi [Security] seadeks [None] ja loote ühenduse pääsupunktiga, ei krüpteerita kaamera ja pääsupunkti vahelist traadita sidet ning muu osapool võib selle signaali levialas kinni püüda. Kasutage turvalisuse suurendamiseks WPA2 või WPA3 turvaprotokolli.
- SONY EI VASTUTA MIS TAHES KAHJUDE EEST, MILLE PÕHJUS ON VAJALIKE TURVAMEETMETE MITTEKASUTAMINE EDASTUSSEADMETE PUHUL, VÄLTIMATUTE ANDMELEKETE EEST, MIS ON TINGITUD EDASTUSE TEHNILISTEST ANDMETEST, VÕI MIS TAHES TURBEPROBLEEMIDE EEST.
- Olenevalt kasutuskeskkonnast võivad volitusteta kolmandad osapooled võrgu kaudu seadmele juurde pääseda. Tagage seadme ühendamisel võrguga, et võrk on korralikult kaitstud.
- Toote võrguga ühendamisel tuleb teha seda sellise süsteemi kaudu, mis pakub kaitsefunktsiooni, nagu ruuter või tulemüür. Kui ühendate ilma kaitseta, võib tekkida turbeprobleeme.

TP1002220976

MPC-2610
Turvalisuse ettevaatusabinõud

Internetiühenduse ettevaatusabinõud

Selles teemas kirjeldatakse seadme internetiga ühendamise ettevaatusabinõusid.

- Seade ei saa luua traadita kohtvõrgu kaudu ühendust pääsupunktiga, mis kasutab ainult WEP-d või WPA-d, kuna need on nõrkustega turvaseaded.
- See seade ei ole võrguseade (nt marsruuter või kommutaator). Seade on tungivalt soovitatav ühendada võrguga, kus saate võrguseadeid nõuetekohaselt konfigureerida ja hallata, et tagada kaitse võrgurünnete vastu (nt teenusetõkestusründed).
- Ühendage seade võrguga õigesti konfigureeritud ja hallatud marsruuteri kaudu või ühendage see sama funktsiooniga LAN-pordiga. Kui ühendus luuakse ilma selle kaitseta (nt kasutades tasuta Wi-Fi-võrku), võib esineda turvaprobleeme. Kui marsruuterid on õigesti konfigureeritud, pakuvad need teenusetõkestusrünnete või seadmete talitlushäirete vastu võrgus piisavat kaitset. Kui märkate midagi ebatavalist, ühendage kaamera kohe võrgust lahti.

TP1002220977

MPC-2610
Turvalisuse ettevaatusabinõud

Võrgufunktsiooniga seotud ettevaatusabinõud

Selles teemas kirjeldatakse seadme võrgufunktsiooni ettevaatusabinõusid.

- Kui tuvastatakse volitamata juurdepääs, võib ühendus kaameraga katkeda. Sellisel juhul looge ühendus algusest peale uuesti.
- Seadme ühendamise autentimisteave kuvatakse, kui kasutate menüüd [Network] – [Network Setup] – [Show Authentication]. Jälgige, et teised ei saaks ekraanikuva vaadata ega QR-koodi pilti kopeerida.
- Kasutajanimi ja parool tuleb sisestada ostmise ajal. Kasutajanime ja parooli seadistamisel veenduge, et seaded ei oleks teistele nähtavad. Määrake kasutajanimi ja parool järgmiselt.

[User Name]	– Määrake kasutajanimi, mis sisaldab 1 kuni 16 tähemärki. – Tehase vaikeseadistus on „admin“. – Kasutada on lubatud järgmisi tähemärke. Tähed (suur- ja väiketähed), numbrid, sümbolid (! % + , - . = _)
[Password]	– Määrake parool, mis sisaldab 8 kuni 16 tähemärki, sealhulgas vähemalt 1 tähte ja vähemalt 1 numbrit. – Kasutada on lubatud järgmisi tähemärke. Tähed (suur- ja väiketähed), numbrid, sümbolid (! % + , - . = _)

TP1002220978

MPC-2610
Turvalisuse ettevaatusabinõud

Traadita kohtvõrguga (LAN) seotud ettevaatusabinõud

Selles teemas kirjeldatakse seadme traadita kohtvõrgu kaudu ühendamise ettevaatusabinõusid.

- Selle seadme abijuhendis viidatakse LAN-ühendusi vahendatavatele traadita kohtvõrgu pääsupunktidele ja traadita kohtvõrgu marsruuteritele kui „pääsupunktidele”.
- Suvandi [Security] (krüpteerimismeetod) seadeks saab määrata [None], [WPA2] või [WPA3]. Turvalisuse seisukohalt on soovitatav kasutada seadet [WPA2] või [WPA3]. Kui valitud on [None], kuvatakse enne ühendamist teade. Turvalise traadita LAN-ühenduse loomiseks on tungivalt soovitatav luua ühendus WPA2 või WPA3 turvaseadega pääsupunktidega.
- Vaikimisi valitakse turvaseade WPA2, kui registreerite traadita LAN-ühenduse pääsupunkti, kasutades suvandit [Manual Register].
- Kui loote pääsupunktiga ühenduse ilma turvaseadeta, ohustab teid nõrkuste korral häkkimine, muude osapoolte pahatahtlik juurdepääs või ründed. Kui seda on võimalik vältida, siis turvaseadeta ühenduse kasutamine pole soovitatud.
- Traadita kohtvõrgu turvalisuse konfigureerimine on väga tähtis. Sony ei vastuta kahjude eest, kui turvameetmeid ei ole rakendatud või kui traadita kohtvõrgu kasutamisel ilmneb vältimatute asjaolude tõttu turvaprobleem.

TP1002220979

MPC-2610
Turvalisuse ettevaatusabinõud

USB-lõastamisega seotud ettevaatusabinõud

Selles teemas kirjeldatakse seadme USB-lõastamise kaudu ühendamise ettevaatusabinõusid.

- Kasutage lõastamiseks ainult usaldusväärseid nutitelefone. Tundmatu päritoluga seadmete ühendamine ei ole turvakaalutlustel soovitatav.

TP1002220980

Teave FTPES (FTPS)-funktsiooni kohta

FTPS-funktsioon toetab turvalise failiedastuse tagamiseks eri krüpteerimisalgoritme. Paljude eri serveritega ühilduvuse tagamiseks on toetatud mitmed krüpteerimisalgoritmid, millest mõned ei pruugi praeguste turvalisuse heade tavadega vastavuses olla.

FTPS-funktsiooni toetatud krüpteerimisalgoritmid

Toetatud on järgmised krüpteerimisalgoritmid.

- 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

Soovitatud krüpteerimisalgoritmid

NIST-i soovituste (NIST SP 800-57 osa 1, parandus 5) ja seotud turbestandardite põhjal soovitatakse järgmisi krüpteerimisalgoritme.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Teave iganenud algoritmide kohta

FTPS-funktsioon toetab ühilduvuse puhul ka järgmisi algoritme, kuid need on NIST-i soovituste (NIST SP 800-57 osa 1, parandus 5) ja seotud turbestandardite põhjal iganenud ning võidakse tulevases versioonis eemaldada.

- 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

Teave ühenduse ühilduvuse kohta

FTPS-funktsioon on loodud turvalisuse ja ühilduvuse tasakaalu silmas pidades. Praegu on iganenud algoritmid toetatud järgmistel põhjustel, kuid need võidakse tulevases versioonis turvalisuse suurendamiseks eemaldada.

- Vabakutselised foto- ja videograafid peavad loom ühenduse eri klientarvutites töötavate serveritega.
- Ühilduvus vanemate süsteemide ja pärandserveritega tuleb säilitada.
- Kõik kasutajad ei ole valmis turvalisemale seadistustele üle minema, kuna serveri pool on krüpteerimisalgoritmi seadete muutmine keeruline.
- FTPS-i seadeid jagatakse sageli muude turbeteenustega. Kõiki muudatusi tuleb hoolikalt kaaluda, kuna need võivad mõjutada muid serveri teenuseid.
- Vaja on väga mitmesuguste krüpteerimisalgoritmide tuge, et tagada eri keskkondades koostalitlusvõime.

FTPS-ühenduse ajal kasutatav krüpteerimisalgoritm määratletakse sihtserveriga automaatse kooskõlastuse kaudu ja oleneb seetõttu serveri seadetest. Turvariskidest ollakse küll teadlik, kuid hetkel on prioriteet rahuldada kasutajate mitmekülgsed vajadused.

Turvariskid

Iganenud algoritmide (sh CBC/DHE/RSA/SHA-1) kasutamine suurendab ohtu, et ründaja võib krüpteeritud andmed dekrüpteerida või neid manipuleerida, seades andmed edastuse ajal ohtu.

Turvalise ühenduse soovitused

Enne FTPS-funktsiooni kasutamist kontrollige, kas ühenduse sihtserver toetab soovitatud krüpteerimisalgoritmi. Lubage server pool ainult soovitatud algoritmid ja keelake iganenud algoritmid.

Üleslaadimine turvalise FTP kaudu

Failid saate laadida üles krüpteeritult, kasutades FTPS-i Explicit-režiimis (FTPES), et luua ühendus failide sihtserveriga. Turvalise FTP-edastuse jaoks määrake failiedastusserveri sätetes suvandi [Using Secure Protocol] seadeks [On] ja importige sertifikaat.

Viited

- 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 (hõlmab värskendusi alates 10.06.2016).

Sertifikaat

Kirjutage FTPES (FTPS)-funktsiooni kasutatav sertifikaat mälukaardi juurkausta. Määrake faili nimi järgmiselt: certification.pem (PEM-vorming)
Laaditava sertifikaadi maksimaalne suurus on 1 MB.

TP1002220981