ILME-FX6

Drošības pasākumi

Šajā palīdzības pamācībā ir aprakstīti failu pārsūtīšanas un straumēšanas drošības pasākumi, izmantojot ierīci.

ILME-FX6
Drošības pasākumi

Drošības pasākumi

Šajā tēmā ir aprakstīti piesardzības pasākumi, pievienojot ierīci tīklam.

- Signālu tuvumā komunikācijas saturu var nejauši pārtvert nepilnvarotas trešās personas. Izmantojot bezvadu LAN komunikāciju, veiciet pareizus drošības pasākumus, lai aizsargātu komunikācijas saturu.
- Ja iestatāt [Security] bezvadu LAN iestatījumu uz [None] izveidojiet savienojumu ar piekļuves punktu, bezvadu sakari starp kameru un piekļuves punktu netiks šifrēti, un signāla diapazonā tos var pārtvert trešā persona. Papildu drošībai izmantojiet WPA2 vai WPA3 drošības protokolu.
- SONY NEUZŅEMAS ATBILDĪBU PAR JEBKĀDIEM BOJĀJUMIEM, KAS RADUŠIES, NEPIEMĒROJOT ATBILSTOŠUS DROŠĪBAS LĪDZEKĻUS DATU PĀRRAIDES IERĪCĒS, NENOVĒRŠAMĀM DATU NOPLŪDĒM, KAS RADUŠĀS PĀRRAIDES SPECIFIKĀCIJU VAI JEBKĀDU DROŠĪBAS PROBLĒMU REZULTĀTĀ.
- Atkarībā no darbības vides neautorizētas trešās puses tīmeklī var piekļūt ierīcei. Savienojot ierīci ar tīklu, pārliecinieties, vai tīkls ir atbilstoši aizsargāts.
- Pievienojiet šo produktu tīklam, izmantojot sistēmu, kas nodrošina aizsardzības funkciju, piemēram, rūteri vai ugunsmūri. Pievienojot bez šādas aizsardzības, ir iespējamas ar drošību saistītas problēmas.

TP1002274542

ILME-FX6
Drošības pasākumi

Interneta savienojuma piesardzības pasākumi

Šajā tēmā ir aprakstīti piesardzības pasākumi, veidojot ierīces savienojumu ar internetu.

- Ierīce nevar izveidot bezvadu LAN savienojumu ar piekļuves punktu, kas izmanto tikai WEP vai WPA — tās ir drošības metodes, kurām ir nepilnības.
- Ierīce nav tīkla ierīce (piemēram, maršrutētājs vai komutēšanas centrmezgls). Ļoti ieteicams ierīci savienot ar tīklu, kurā var atbilstoši konfigurēt un pārvaldīt tīkla iestatījumus, lai aizsargātu tīklu pret uzbrukumiem, piemēram, DoS uzbrukumiem (pakalpojumatteices uzbrukumiem).
- Pievienojot ierīci tīklam, savienojiet to, izmantojot maršrutētāju, kas ir atbilstoši konfigurēts un pārvaldīts, vai pievienojiet to LAN portam ar tādu pašu funkcionalitāti. Ja savienojums ir izveidots bez šādas aizsardzības (piemēram, izmantojot bezmaksas Wi-Fi), var rasties drošības problēmas. Ja maršrutētāji ir pareizi konfigurēti, tie nodrošina pietiekamu aizsardzību pret DoS uzbrukumiem vai ierīču funkcionalitātes zudumu tīklā. Ja pamanāt kaut ko neparastu, nekavējoties atvienojiet kameru no tīkla.

TP1002274543

Ar tīkla funkciju saistītie piesardzības pasākumi

Šajā tēmā ir aprakstīti piesardzības pasākumi saistībā ar ierīces tīkla funkciju.

- Ja tiek konstatēta nesankcionēta piekļuve, kamera var nespēt akceptēt komunikāciju. Ja tā notiek, atkārtoti izveidojiet savienojumu no sākuma.
- Nospiediet pogu [Show Authentication] statusa ekrānā [Network], lai parādītu autentifikācijas informāciju savienojuma izveidei ar ierīci. Uzmanieties, lai ekrānu nevarētu redzēt un citi nevarētu nokopēt QR koda attēlu.
- Lietotājvārds un parole tiek automātiski ģenerēti un iestatīti kamerā iegādes brīdī. Iestatot lietotājvārdu un paroli, pārliecinieties, vai iestatījumi nav redzami citiem lietotājiem. Vārdu un paroli iestatiet šādi.

[User Name]	– Iestati lietotājvārdu, kas sastāv no 1 līdz 16 rakstzīmēm. – Ražotāja noklusējumā tas ir iestatīts kā “admin”. – Tālāk ir norādītas derīgas ievadāmās rakstzīmes. Alfabēta rakstzīmes (lielās un mazās), ciparu rakstzīmes, simboli (! % + , - . = _)
[Password]	– Iestati paroli, kas sastāv no 8 līdz 16 rakstzīmēm, no kurām vismaz 1 ir burtzīme un vismaz 1 ir cipars. – Tālāk ir norādītas derīgas ievadāmās rakstzīmes. Alfabēta rakstzīmes (lielās un mazās), ciparu rakstzīmes, simboli (! % + , - . = _)

TP1002274544

ILME-FX6
Drošības pasākumi

Ar bezvadu LAN saistītie piesardzības pasākumi

Šajā tēmā ir aprakstīti piesardzības pasākumi, veidojot ierīces savienojumu ar bezvadu LAN.

- Šīs ierīces palīdzības pamācībā bezvadu LAN piekļuves punkti un bezvadu LAN maršrutētāji, kas nodrošina LAN savienojumus, tiek saukti par “piekļuves punktiem”.
- [Security] (šifrēšanas metode) var iestatīt uz [None], [WPA2] vai [WPA3]. No drošības viedokļa ir ieteicama [WPA2] vai [WPA3] lietošana. Ja ir atlasīts [None], pirms savienojuma izveides tiek parādīts ziņojums. Lai izveidotu drošu bezvadu LAN savienojumu, ļoti ieteicams izveidot savienojumu ar piekļuves punktiem, izmantojot drošības iestatījumu WPA2 vai WPA3.
- Kad reģistrējat bezvadu LAN piekļuves punktu, izmantojot [Manual Register], pēc noklusējuma ir atlasīta WPA2 drošības metode.
- Ja izveidojat savienojumu ar piekļuves punktu bez drošības iestatījumiem, iespējama uzlaušana, ļaunprātīga trešo personu piekļuve vai uzbrukumi vājajām vietām. Ja vien tas nav neizbēgami, savienojuma izveide bez jebkādiem drošības iestatījumiem nav ieteicama.
- Bezvadu LAN drošības konfigurēšana ir ļoti svarīga. Uzņēmums Sony neuzņemas atbildību par zaudējumiem, kas radušies drošības pasākumu neveikšanas dēļ vai drošības problēmu dēļ, kas saistās ar nenovēršamiem bezvadu LAN lietošanas apstākļiem.

TP1002274545

Piesardzības pasākumi, kas saistīti ar USB piesaisti

Šajā tēmā ir aprakstīti piesardzības pasākumi, veidojot ierīces savienojumu ar USB piesaisti.

- Piesaistei izmantojiet tikai uzticamas viedtālruņa ierīces. Drošības apsvērumu dēļ nav ieteicams izveidot savienojumu ar nezināmas izcelsmes ierīcēm.

TP1002274546

Par funkciju FTPES (FTPS)

FTPS funkcija atbalsta dažādus šifrēšanas algoritmus, lai nodrošinātu drošu failu pārsūtīšanu. Saderībai ar plašu serveru klāstu tiek atbalstīti vairāki šifrēšanas algoritmi, no kuriem daži, iespējams, neatbilst pašreizējai drošības paraugpraksei.

Šifrēšanas algoritmi, ko atbalsta FTPS funkcija

Tiek atbalstīti šādi šifrēšanas algoritmi.

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- 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

Ieteicamie šifrēšanas algoritmi

Pamatojoties uz NIST ieteikumiem (NIST SP 800-57 1. daļas 5. redakcija) un saistītajiem drošības standartiem, ieteicams izmantot šādus šifrēšanas algoritmus.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Par novecojušiem algoritmiem

FTPS funkcija atbalsta arī tālāk norādītos saderības algoritmus, tomēr, pamatojoties uz NIST ieteikumiem (NIST SP 800-57 1. daļas 5. pārskatījums) un saistītajiem drošības standartiem, tie ir novecojuši, un nākamajā versijā tie var tik noņemti.

- 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

Par savienojuma saderību

FTPS funkcija ir izstrādāta, ņemot vērā drošības un saderības līdzsvaru. Pašlaik novecojuši algoritmi tiek atbalstīti tālāk norādīto iemeslu dēļ, bet, lai uzlabotu drošību, tie var tikt noņemti nākamajā versijā.

- Ārštata fotogrāfiem un videogrāfiem ir jāveido savienojums ar serveriem, kas darbojas pie dažādiem klientiem.
- Ir jāsaglabā saderība ar vecākām sistēmām un mantotajiem serveriem.
- Ne visi lietotāji ir gatavi pāriet uz drošāku iestatījumu, jo šifrēšanas algoritma iestatījumu maiņa servera pusē ir sarežģīta.
- FTPS iestatījumi bieži tiek koplietoti ar citiem drošiem pakalpojumiem. Jebkuras izmaiņas ir rūpīgi jāapsver, jo tās var ietekmēt citus servera pakalpojumus.
- Lai nodrošinātu sadarbspēju dažādās vidēs, ir jāatbalsta plašs šifrēšanas algoritmu klāsts.

Šifrēšanas algoritmu, kas tiek izmantots FTPS savienojuma laikā, nosaka automātiska vienošanās ar galamērķa serveri, tādēļ tas ir atkarīgs no servera iestatījumiem. Lai gan ir apzināti drošības riski, šobrīd tiek prioritizēta saderība, lai apmierinātu dažādās lietotāju vajadzības.

Drošības riski

Novecojušu algoritmu, tostarp CBC/DHE/RSA/SHA-1, izmantošana palielina risku, ka uzbrucējs var atšifrēt vai sagrozīt šifrētus datus, piekļūstot datiem pārsūtīšanas laikā.

Ieteikums drošam savienojumam

Pirms FTPS funkcijas izmantošanas pārbaudiet, vai savienojuma mērķa serveris atbalsta ieteicamo šifrēšanas algoritmu. Iespējojiet tikai ieteicamos algoritmus servera pusē un atspējojiet novecojušos algoritmus.

Augšupielāde, izmantojot drošu FTP

Šifrētus failus varat augšupielādēt, savienojumam ar galamērķa faila serveri izmantojot FTPS eksplicītajā režīmā (FTPES).
Lai nodrošinātu drošu FTP pārsūtīšanu, failu pārsūtīšanas galamērķa servera iestatījumos [Using Secure Protocol] iestatiet uz [On] un importējiet sertifikātu.

Atsauces

- 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 (ietver atjauninājumus uz 06.10.2016.).

Sertifikāts

Ierakstiet sertifikātu, ko izmanto funkcija FTPES (FTPS), atmiņas kartes saknes direktorijā. Iestatiet faila nosaukumu šādi.
certification.pem (PEM formāts)
Maksimālais sertifikāta lielums, ko var ielādēt, ir 1 MB katram sertifikātam.

TP1002274547