MPC-2610

Sikkerhedsforanstaltninger

Denne vejledning til hjælp beskriver sikkerhedsforanstaltninger for filoverførsel og streaming ved brug af enheden.

MPC-2610
Sikkerhedsforanstaltninger

Sikkerhedsforanstaltninger

Dette emne beskriver sikkerhedsforanstaltninger, når enheden forbindes til et netværk.

- Kommunikationsindhold kan, uden at du ved det, blive opsnappet af uautoriserede tredjeparter i nærheden af signalerne. Når trådløs LAN-kommunikation anvendes, skal der implementeres sikkerhedsforanstaltninger på behørig vis for at beskytte kommunikationsindholdet.
- Hvis indstillingen for [Security] i det trådløse LAN-netværk indstilles til [None], og kameraet forbindes til et adgangspunkt, vil den trådløse kommunikation mellem kameraet og adgangspunktet ikke være krypteret, og den vil muligvis kunne opfanges af en tredjepart, der befinder sig inden for signalets rækkevidde. Brug en af sikkerhedsprotokollerne WPA2 eller WPA3 for at opnå forbedret sikkerhed.
- SONY ER IKKE ANSVARLIG FOR NOGEN FORM FOR SKADE FORÅRSAGET AF MANGLENDE OVERHOLDELSE AF SIKKERHEDSFORHOLDSREGLER PÅ TRANSMISSIONSENHEDER, UUNDGÅELIGE DATALÆK FORÅRSAGET AF TRANSMISSIONSSPECIFIKATIONER ELLER ENHVER TYPE SIKKERHEDSPROBLEMER.
- Afhængigt af driftsmiljøet kan uautoriserede tredjeparter på netværket have adgang til enheden. Når enheden tilsluttes til netværket, skal du sørge for at bekræfte, at netværket er sikkert beskyttet.
- Når dette produkt kobles på et netværk, skal opkoblingen ske via et system med en beskyttelsesfunktion, som f.eks. en router eller firewall. Hvis opkoblingen sker uden en sådan beskyttelse, kan der opstå sikkerhedsproblemer.

TP1002220960

MPC-2610
Sikkerhedsforanstaltninger

Forholdsregler vedrørende internetforbindelse

Dette emne beskriver forholdsregler, når enheden forbindes til internettet.

- Enheden kan ikke oprette forbindelse via et trådløst LAN til et adgangspunkt, der kun benytter WEP eller WPA, da disse sikkerhedsprotokoller har sårbarheder.
- Enheden er ikke en netværksenhed (for eksempel en router eller switch). Det anbefales kraftigt at forbinde enheden til et netværk, hvor netværksindstillingerne kan konfigureres og administreres på passende vis, så enheden kan beskyttes mod netværksbaserede angreb såsom DoS-angreb (Denial of Service-angreb).
- Når enheden forbindes til et netværk, skal det ske via en router, der er konfigureret og administreres på passende vis, eller via en LAN-port, der har samme funktionalitet. Hvis den forbindes uden denne beskyttelse (for eksempel ved brug af gratis wi-fi), kan det medføre sikkerhedsproblemer. Når en router er korrekt konfigureret, giver den tilstrækkelig beskyttelse mod DoS-angreb og tab af funktionalitet for enheder i netværket. Hvis der bemærkes noget usædvanligt, skal kameraets forbindelse til netværket straks afbrydes.

TP1002220961

MPC-2610
Sikkerhedsforanstaltninger

Forholdsregler vedr. netværksfunktionen

Dette emne beskriver forholdsregler om enhedens netværksfunktion.

- Hvis der registreres uautoriseret adgang, kan kameraet muligvis ikke acceptere kommunikation. Hvis dette sker, skal du starte forfra med at oprette forbindelse.
- Godkendelsesoplysningerne for tilslutning til enheden vises, når du bruger [Network] – [Network Setup] – [Show Authentication]. Pas på, at skærmen ikke kan ses, og at QR-kodebilledet ikke kan kopieres af andre.
- Der skal indstilles et brugernavn og en adgangskode på købstidspunktet. Når du indstiller brugernavn og adgangskode, skal du sørge for, at indstillingerne ikke er synlige for andre. Angiv brugernavnet og adgangskoden som følger.

[User Name]	– Angiv et brugernavn, der består af 1 til 16 tegn. – Dette er som standard "admin". – Følgende er gyldige tegn. Alfabetiske tegn (store og små bogstaver), numeriske tegn, symboler (! % + , - . = _)
[Password]	– Angiv en adgangskode, der består af 8 til 16 tegn, og som indeholder mindst 1 eller flere alfabetiske tegn og 1 eller flere numeriske tegn. – Følgende er gyldige tegn. Alfabetiske tegn (store og små bogstaver), numeriske tegn, symboler (! % + , - . = _)

TP1002220962

MPC-2610
Sikkerhedsforanstaltninger

Forholdsregler vedr. trådløst LAN

Dette emne beskriver forholdsregler, når enheden forbindes via trådløst LAN.

- I vejledningen til hjælp for denne enhed omtales trådløse LAN-adgangspunkter og trådløse LAN-routere, der videreformidler LAN-forbindelser, som "adgangspunkter".
- [Security] (krypteringsmetode) kan indstilles til [None], [WPA2] eller [WPA3]. Af hensyn til sikkerheden anbefales det at anvende [WPA2] eller [WPA3]. Når [None] er valgt, vises en besked, før der oprettes forbindelse. For at opnå en sikker trådløs LAN-forbindelse anbefales det kraftigt at oprette forbindelse til adgangspunkter med WPA2- eller WPA3-sikkerhed.
- Som standard er WPA2-sikkerhed valgt, når der registreres et trådløst LAN-adgangspunkt ved brug af [Manual Register].
- Hvis du opretter forbindelse til et adgangspunkt uden sikkerhed, kan du blive udsat for hacking, at ondsindede tredjeparter får adgang, eller angreb på sårbarheder. Medmindre det er uundgåeligt, frarådes det at oprette forbindelse uden sikkerhed.
- Konfigurering af sikkerhed på et trådløst LAN er meget vigtigt. Sony kan ikke holdes ansvarlig for eventuelle skader, der skyldes, at der ikke er truffet sikkerhedsforanstaltninger, eller hvis der opstår et sikkerhedsproblem på grund af uundgåelige omstændigheder ved brug af trådløst LAN.

TP1002220963

MPC-2610
Sikkerhedsforanstaltninger

Forholdsregler vedr. USB-forankring

Dette emne beskriver forholdsregler, når enheden forbindes via USB-forankring.

- Opret kun kabelforbindelse til smartphones, du har tillid til. Af hensyn til sikkerheden frarådes det at oprette forbindelse til enheder af ukendt oprindelse.

TP1002220964

Om FTPES (FTPS)-funktionen

FTPS-funktionen understøtter forskellige krypteringsalgoritmer, der muliggør sikker filoverførsel. Flere krypteringsalgoritmer understøttes for at sikre kompatibilitet med en bred vifte af servere, men nogle af algoritmerne overholder muligvis ikke de nuværende bedste sikkerhedspraksisser.

Krypteringsalgoritmer understøttet af FTPS-funktionen

Følgende krypteringsalgoritmer understøttes.

- 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

Anbefalede krypteringsalgoritmer

Følgende krypteringsalgoritmer anbefales baseret på NIST-anbefalingerne (NIST SP 800-57 Part 1 Revision 5) og relaterede sikkerhedsstandarder.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Om forældede algoritmer

FTPS-funktionen understøtter også følgende algoritmer af hensyn til kompatibilitet, men de er forældede baseret på NIST-anbefalingerne (NIST SP 800-57 Part 1 Revision 5) og relaterede sikkerhedsstandarder og kan blive fjernet i en fremtidig version.

- 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

Om forbindelseskompatibilitet

FTPS-funktionen er udviklet med henblik på balance mellem sikkerhed og kompatibilitet. I øjeblikket understøttes forældede algoritmer af følgende årsager, men de kan blive fjernet i en fremtidig version for at forbedre sikkerheden.

- Freelancefotografer og -videografer skal kunne oprette forbindelse til servere, der kører på forskellige klienter.
- Kompatibilitet med ældre systemer og ældre servere skal opretholdes.
- Ikke alle brugere er klar til at skifte til en mere sikker indstilling, da det er kompliceret at ændre krypteringsalgoritmen på serversiden.
- FTPS-indstillingerne deles ofte med andre sikre tjenester. Alle ændringer bør overvejes nøje, da de kan have en indvirkning på andre tjenester på serveren.
- En bred vifte af krypteringsalgoritmer skal understøttes for at sikre interoperabilitet i forskellige miljøer.

Den krypteringsalgoritme, der bruges under en FTPS-forbindelse, bestemmes ved automatisk forhandling med destinationsserveren og afhænger derfor af serverindstillingerne. Selvom sikkerhedsrisiciene er kendte, prioriteres kompatibilitet i øjeblikket for at imødekomme brugernes forskellige behov.

Sikkerhedsrisici

Brug af forældede algoritmer, herunder CBC/DHE/RSA/SHA-1, øger risikoen for, at krypterede data kan blive dekrypteret eller manipuleret af en angriber, så data eksponeres under overførslen.

Anbefaling til sikker forbindelse

Før du bruger FTPS-funktionen, bør du kontrollere, at forbindelsens destinationsserver understøtter den anbefalede krypteringsalgoritme. Aktivér kun de anbefalede algoritmer på serversiden, og deaktivér de forældede algoritmer.

Overførsel ved hjælp af sikker FTP

Du kan overføre filer med kryptering ved brug af FTPS in Explicit mode (FTPES) for forbindelse med destinationsfilserveren.
For sikker FTP-overførsel skal du indstille [Using Secure Protocol] til [On] i indstillingerne for filoverførselsdestinationsserveren og importere et certifikat.

Referencer

- 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 (inkluderer opdateringer pr. 10/06/2016).

Certifikat

Skriv certifikatet brugt af FTPES (FTPS)-funktionen til rodmappen på et hukommelseskort. Angiv filnavnet som følger.
certification.pem (PEM-format)
Den maksimale certifikatstørrelse, der kan indlæses, er 1 MB pr. certifikat.

TP1002220965