MPC-2610

Sikkerhetstiltak

Denne hjelpveiledningen beskriver sikkerhetstiltak for filoverføring og strømming ved bruk av enheten.

MPC-2610
Sikkerhetstiltak

Sikkerhetstiltak

Dette emnet beskriver forsiktighetsregler når du kobler enheten til et nettverk.

- Kommunikasjonsinnhold kan bli fanget opp av uautoriserte tredjeparter i nærheten av signalene, uten at vi kjenner til det. Når man benytter trådløs LAN-kommunikasjon skal det iverksettes sikkerhetstiltak for å beskytte kommunikasjonsinnholdet.
- Hvis du angir [Security]-innstillingen for trådløst LAN til [None] og kobler til et tilgangspunkt, vil ikke trådløs kommunikasjon mellom kameraet og tilgangspunktet være kryptert og kan bli registrert av en tredjepart innenfor rekkevidden til signalet. Bruk WPA2- eller WPA3-sikkerhetsprotokollen for økt sikkerhet.
- SONY SKAL IKKE VÆRE ANSVARLIG FOR SKADER AV NOE SLAG SOM FØLGER AV UNNLATELSE AV Å IMPLEMENTERE RIKTIGE SIKKERHETSTILTAK PÅ OVERFØRINGSENHETER, UUNNGÅELIGE DATALEKKASJER PÅ GRUNN AV OVERFØRINGSSPESIFIKASJONER ELLER SIKKERHETSPROBLEMER AV NOE SLAG.
- Avhengig av driftsmiljøet, kan uautoriserte tredjeparter på nettverket være i stand til å få tilgang til enheten. Ved tilkobling av enheten til nettverk må du sørge for å kontrollere at nettverket har sikker beskyttelse.
- Ved tilkobling av dette produktet til et nettverk, koble til via et system som har en beskyttelsesfunksjon, som for eksempel en ruter eller en brannvegg. Hvis produktet kobles til uten slik beskyttelse kan det medføre sikkerhetsproblemer.

TP1002221041

MPC-2610
Sikkerhetstiltak

Forsiktighetsregler tilkobling til Internett

Dette emnet beskriver forsiktighetsregler når du kobler enheten til et Internett.

- Enheten kan ikke koble til via trådløst LAN til et tilgangspunkt som bare bruker WEP eller WPA, som er sikkerhetsmetoder som har sårbarheter.
- Enheten er ikke en nettverksenhet (for eksempel en ruter eller svitsjhub). Det anbefales sterkt å koble enheten til et nettverk der du kan konfigurere og administrere nettverksinnstillingene på riktig måte for å beskytte mot nettverksbaserte angrep, for eksempel DoS-angrep (Denial of Service).
- Når du kobler enheten til et nettverk, koble den til via en ruter som er konfigurert og administrert på riktig måte, eller koble den til en LAN-port som har samme funksjonalitet. Hvis tilkoblet uten slik beskyttelse (for eksempel ved bruk av gratis Wi-Fi), kan det oppstå sikkerhetsproblemer. Når de er riktig konfigurert, gir rutere tilstrekkelig beskyttelse mot DoS-angrep eller tap av funksjonalitet til enheter i nettverket. Hvis du oppdager noe uvanlig, koble kameraet umiddelbart fra nettverket.

TP1002221042

MPC-2610
Sikkerhetstiltak

Forsiktighetsregler knyttet til nettverksfunksjonen

Dette emnet beskriver forsiktighetsregler for enhetens nettverkfunksjon.

- Hvis uautorisert tilgang oppdages, kan kameraet bli ute av stand til å akseptere kommunikasjon. Hvis dette skjer, koble til fra begynnelsen.
- Autentiseringsinformasjonen for tilkobling til enheten vises når du bruker [Network] – [Network Setup] – [Show Authentication]. Sørg for at skjermen ikke vises for andre og at QR-kodebildet ikke kan kopieres av andre.
- Et brukernavn og passord må angis ved kjøp. Når du angir brukernavn og passord, sørg for at innstillingene ikke er synlige for andre. Angi brukernavn og passord som følger.

[User Name]	– Angi et brukernavn som består av 1 til 16 tegn. – Dette er satt til "admin" som standard fra fabrikken. – Følgende er gyldige inndatategn. Alfabetiske tegn (store og små bokstaver), tall, symboler (! % + , - . = _)
[Password]	– Angi et passord som består av 8 til 16 tegn, og som inneholder minst 1 eller flere alfabetiske tegn og 1 eller flere numeriske tegn. – Følgende er gyldige inndatategn. Alfabetiske tegn (store og små bokstaver), tall, symboler (! % + , - . = _)

TP1002221043

MPC-2610
Sikkerhetstiltak

Forsiktighetsregler knyttet til trådløst LAN

Dette emnet beskriver forsiktighetsregler ved tilkobling av enheten via trådløst LAN.

- I hjelpveiledningen for denne enheten blir trådløse LAN-tilgangspunkter og trådløse LAN-rutere som videresender LAN-tilkoblinger referert til som "tilgangspunkter".
- [Security] (krypteringsmetode) kan angis til [None], [WPA2] eller [WPA3]. Bruk av [WPA2] eller [WPA3] anbefales fra et sikkerhetssynspunkt. Når [None] er valgt, vises en melding før tilkobling. For sikker trådløs LAN-tilkobling anbefales tilkobling til tilgangspunkter med WPA2- eller WPA3-sikkerhetsinnstilling på det sterkeste.
- Som standard er WPA2-sikkerhetsmetoden valgt når du registrerer trådløst tilgangspunktet for trådløst LAN med [Manual Register].
- Hvis du kobler til et tilgangspunkt uten noen sikkerhetsinnstilling, kan du bli utsatt for hacking, tilgang fra ondsinnede tredjeparter eller angrep på sårbarheter. Med mindre det ellers er uunngåelig, anbefales ikke tilkobling uten noen sikkerhetsinnstilling.
- Konfigurering av sikkerhet på et trådløst LAN er svært viktig. Sony vil ikke holdes ansvarlig for skader som følge av at sikkerhetstiltak ikke er iverksatt, eller hvis det oppstår et sikkerhetsproblem på grunn av uunngåelige omstendigheter ved bruk av trådløst LAN.

TP1002221044

MPC-2610
Sikkerhetstiltak

Forsiktighetsregler for Internett-deling via USB

Dette emnet beskriver forsiktighetsregler ved tilkobling av enheten gjennom Internett-deling via USB.

- Bruk bare pålitelige smarttelefonenheter for deling. På grunn av sikkerhetshensyn anbefales det ikke å koble til enheter av ukjent opprinnelse.

TP1002221045

Om FTPES (FTPS)-funksjonen

FTPS-funksjonen støtter ulike krypteringsalgoritmer for å sikre sikker filoverføring. Flere krypteringsalgoritmer, hvorav noen kanskje ikke samsvarer med gjeldende beste praksis for sikkerhet, støttes for kompatibilitet med et bredt spekter av servere.

Krypteringsalgoritmer støttet av FTPS-funksjonen

Følgende krypteringsalgoritmer støttes.

- 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

Anbefalte krypteringsalgoritmer

Følgende krypteringsalgoritmer anbefales basert på NIST-anbefalingene (NIST SP 800-57 del 1 revisjon 5) og relaterte sikkerhetsstandarder.

- 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 utdaterte algoritmer

FTPS-funksjonen støtter også følgende algoritmer for kompatibilitet, men de er avviklet basert på NIST-anbefalingene (NIST SP 800-57 del 1 revisjon 5) og relaterte sikkerhetsstandarder, og kan bli fjernet i en fremtidig versjon.

- 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 tilkoblingskompatibilitet

FTPS-funksjonen er designet med en balanse mellom sikkerhet og kompatibilitet. Foreløpig støttes utdaterte algoritmer av følgende årsaker, men de kan bli fjernet i en fremtidig versjon for å forbedre sikkerheten.

- Frilansfotografer og videografer må koble til servere som kjører på ulike klienter.
- Kompatibilitet med eldre systemer og eldre servere må opprettholdes.
- Ikke alle brukere er forberedt på å endre til en sikrere innstilling fordi det er komplisert å endre innstillingene for krypteringsalgoritmen på serversiden.
- FTPS-innstillingene deles ofte med andre sikre tjenester. Eventuelle endringer må vurderes nøye, da de kan påvirke andre tjenester på serveren.
- Et bredt spekter av krypteringsalgoritmer må støttes for å sikre interoperabilitet i forskjellige miljøer.

Krypteringsalgoritmen som brukes under en FTPS-tilkobling bestemmes av automatisk forhandling med målserveren og avhenger derfor av serverinnstillingene. Selv om man er klar over sikkerhetsrisikoene, er kompatibilitet for tiden prioritert for å tilfredsstille brukernes ulike behov.

Sikkerhetsrisikoer

Bruk av utdaterte algoritmer, inkludert CBC/DHE/RSA/SHA-1, øker risikoen for at krypterte data kan bli dekryptert eller tuklet med av en angriper, og avsløre data under overføring.

Anbefaling for sikker tilkobling

Før du bruker FTPS-funksjonen, kontroller at målserveren for tilkobling støtter den anbefalte krypteringsalgoritmen. Aktiver bare de anbefalte algoritmene på serversiden og deaktiver de utdaterte algoritmene.

Opplasting ved hjelp av sikker FTP

Du kan laste opp filer med kryptering som bruker FTPS i eksplisitt modus (FTPES) for tilkoblingen til målfilserveren. For sikker FTP-overføring, sett [Using Secure Protocol] til [On] i innstillingene for målserveren for filoverføring, og importer et sertifikat.

Referanser

- 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 oppdateringer per 06.10.2016).

Sertifikat

Skriv sertifikatet som brukes av FTPES-funksjonen (FTPS) til rotkatalogen på et minnekort. Still inn filnavnet som følger.
certification.pem (PEM-format)
Maksimal sertifikatstørrelse som kan lastes er 1 MB per sertifikat.

TP1002221046