ILME-FX6

Sigurnosne mjere opreza

Ovaj Vodič za pomoć opisuje sigurnosne mjere opreza za prijenos datoteka i streaming pomoću uređaja.

ILME-FX6
Sigurnosne mjere opreza

Sigurnosne mjere opreza

Ova tema opisuje mjere opreza prilikom povezivanja uređaja s mrežom.

- Sadržaj komunikacije mogu slučajno presresti neovlaštene treće osobe u blizini signala. Prilikom upotrebe bežične LAN komunikacije, pravilno primijenite sigurnosne mjere kako biste zaštitili sadržaj komunikacije.
- Ako postavite postavku [Security] za bežični LAN na [None] i spojite se na pristupnu točku, bežična komunikacija između kamere i pristupne točke neće biti šifrirana i može je presresti treća osoba unutar dometa signala. Radi veće sigurnosti koristite se sigurnosnim protokolom WPA2 ili WPA3.
- TVRTKA SONY NE SNOSI ODGOVORNOST NI ZA KAKVU ŠTETU KOJA JE NASTALA ZBOG NEPRIMJENJIVANJA PROPISANIH SIGURNOSNIH MJERA NA UREĐAJIMA ZA PRIJENOS PODATAKA, ZA NEIZBJEŽNA CURENJA PODATAKA UZROKOVANA SPECIFIKACIJAMA PRIJENOSA, ILI SIGURNOSNE PROBLEMA BILO KOJE VRSTE.
- Ovisno o radnom okruženju, neovlaštene treće osobe na mreži mogu pristupiti uređaju. Pri povezivanju uređaja s mrežom, pobrinite se da je mreža dobro zaštićena.
- Prilikom povezivanja ovog proizvoda s mrežom, povežite se putem sustava koji pruža zaštitnu funkciju, poput usmjerivača ili vatrozida. Ako se povežete bez takve zaštite, mogu nastati sigurnosni problemi.

TP1002274574

ILME-FX6
Sigurnosne mjere opreza

Mjere opreza za internetsku vezu

Ova tema opisuje mjere opreza prilikom povezivanja uređaja s Internetom.

- Ovaj uređaj ne može se povezati putem bežičnog LAN-a na pristupnu točku koja upotrebljava samo WEP ili WPA, koje su sigurnosne ranjive metode.
- Ovaj uređaj nije mrežni uređaj (na primjer, usmjerivač ili preklopni koncentrator). Izričito se preporučuje da povežete uređaj na mrežu na kojoj možete prikladno konfigurirati i upravljati mrežnim postavkama kako biste se zaštitili od napada temeljenih na mreži, kao što su DoS napadi (napadi uskraćivanja usluge).
- Prilikom povezivanja ovog proizvoda s mrežom, povežite ga putem usmjerivača koji je prikladno konfiguriran i kojim se prikladno upravlja, ili ga povežite na LAN priključak koji ima jednaku funkcionalnost. Ako se povežete bez takve zaštite (na primjer, pri korištenju besplatnim Wi-Fi-jem), mogu se pojaviti sigurnosni problemi. Kada su pravilno konfigurirani, usmjerivači pružaju dovoljnu zaštitu od DoS napada ili gubitka funkcionalnosti uređaja u mreži. Ako primijetite bilo što neuobičajeno, odmah odspojite kameru iz mreže.

TP1002274575

ILME-FX6
Sigurnosne mjere opreza

Mjere opreza u vezi s mrežnom funkcijom

Ova tema opisuje mjere opreza za mrežnu funkciju uređaja.

- Ako se otkrije neovlašteni pristup, kamera možda neće moći primiti komunikacije. Ako se to dogodi, ponovite povezivanje ispočetka.
- Pritisnite gumb [Show Authentication] na statusnom zaslonu [Network] da prikažete podatke za provjeru autentičnosti radi povezivanja s uređajem. Pripazite da se zaslon ne može vidjeti i da ostali ne mogu kopirati sliku QR koda.
- Korisničko ime i lozinka automatski se generiraju i postavljaju na kameri prilikom kupnje. Pri postavljanju korisničkog imena i lozinke, pobrinite se da postavke nisu vidljive ostalima. Postavite korisničko ime i lozinku kako slijedi.

[User Name]	– Postavite korisničko ime koje se sastoji od 1 do 16 znakova. – To je postavljeno na »admin« prema tvornički zadanim postavkama. – Sljedeći znakovi su valjani unosi. Abecedna slova (veliko i malo slovo), brojevi, simboli (! % + , - . = _)
[Password]	– Postavite lozinku koja se sastoji od 8 do 16 znakova, a koji sadržavaju barem 1 ili više slova abecede i 1 ili više brojki. – Sljedeći znakovi su valjani unosi. Abecedna slova (veliko i malo slovo), brojevi, simboli (! % + , - . = _)

TP1002274576

ILME-FX6
Sigurnosne mjere opreza

Mjere opreza u vezi s bežičnim LAN-om

Ova tema opisuje mjere opreza prilikom povezivanja uređaja putem bežičnog LAN-a.

- U Vodiču za pomoć na ovom uređaju, pristupne točke bežičnog LAN-a i usmjerivači bežičnog LAN-a koji prenose LAN veze nazivaju se »pristupne točke«.
- [Security] (način šifriranja) može se postaviti na [None], [WPA2] ili [WPA3]. Upotreba [WPA2] ili [WPA3] preporučuje se sa sigurnosnog stajališta. Ako je odabrano [None] prikazuje se poruka prije povezivanja. Želite li imati sigurnu bežičnu LAN vezu, preporučujemo povezivanje s pristupnim točkama uz sigurnosnu postavku WPA2 ili WPA3.
- Prema zadanim postavkama odabrana je sigurnosna metoda WPA2 pri registriranju pristupne točke bežičnog LAN-a upotrebom [Manual Register].
- Ako se povežete s pristupnom točkom bez ikakvih sigurnosnih postavki, možete biti izloženi hakiranju, pristupu zlonamjernih trećih osoba ili napadima na ranjivosti. Osim ako je neizbježno, ne preporučuje se povezivanje bez ikakvih sigurnosnih postavki.
- Konfiguriranje sigurnosti na bežičnom LAN-u vrlo je važno. Sony neće biti odgovoran za bilo kakvu štetu nastalu zbog nepoduzimanja sigurnosnih mjera ili ako se sigurnosni problem pojavi zbog neizbježnih okolnosti prilikom upotrebe bežične LAN mreže.

TP1002274577

Mjere opreza u vezi s USB dijeljenjem veze

Ova tema opisuje mjere opreza prilikom povezivanja uređaja putem USB dijeljenja veze.

- Za dijeljenje veze koristite se samo pouzdanim pametnim telefonima. Povezivanje s uređajima nepoznatog porijekla ne preporučuje se iz sigurnosnih razloga.

TP1002274578

O FTPES (FTPS) funkciji

FTPS funkcija podržava razne algoritme šifriranja kako bi osigurala siguran prijenos datoteka. Podržano je više algoritama šifriranja, od kojih neki možda nisu u skladu s trenutno najboljim sigurnosnim praksama, radi kompatibilnosti sa širokim rasponom poslužitelja.

Algoritmi šifriranja koje podržava FTPS funkcija

Podržani su sljedeći algoritmi šifriranja.

- 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

Preporučeni algoritmi šifriranja

Sljedeći algoritmi šifriranja preporučuju se na temelju NIST preporuka (NIST SP 800-57 Part 1 Revision 5) i povezanih sigurnosnih standarda.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

O zastarjelim algoritmima

FTPS funkcija podržava i sljedeće algoritme radi kompatibilnosti, ali oni su zastarjeli prema NIST preporukama (NIST SP 800-57 Part 1 Revision 5) i povezanim sigurnosnim standardima te mogu biti uklonjeni u budućoj verziji.

- 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

O kompatibilnosti povezivanja

FTPS funkcija osmišljena je s ravnotežom između sigurnosti i kompatibilnosti. Trenutno su zastarjeli algoritmi podržani iz sljedećih razloga, ali mogu biti uklonjeni u budućoj verziji kako bi se poboljšala sigurnost.

- Samostalni fotografi i videografi trebaju se povezati s poslužiteljima koji rade na različitim klijentima.
- Potrebno je održavati kompatibilnost sa starijim sustavima i naslijeđenim poslužiteljima.
- Nisu svi korisnici spremni prijeći na sigurnije postavke, jer je promjena postavki algoritama šifriranja na strani poslužitelja složena.
- FTPS postavke često se dijele s ostalim sigurnim uslugama. Sve promjene moraju se pažljivo razmotriti, jer mogu utjecati na ostale usluge na poslužitelju.
- Mora biti podržan širok raspon algoritama šifriranja kako bi se osigurala interoperabilnost u različitim okruženjima.

Algoritam šifriranja koji se upotrebljava tijekom FTPS veze određuje se automatskim pregovaranjem s odredišnim poslužiteljem i stoga ovisi o postavkama poslužitelja. Premda smo svjesni sigurnosnih rizika, trenutno se daje prednost kompatibilnosti kako bi se zadovoljile raznolike potrebe korisnika.

Sigurnosni rizici

Upotreba zastarjelih algoritama, uključujući CBC / DHE / RSA / SHA-1, koji su ranjivi tijekom prijenosa, povećava rizik da napadači šifrirane podatke dešifriraju ili neovlašteno izmijene.

Preporuka za sigurnu vezu

Prije upotrebe FTPS funkcije, provjerite podržava li odredišni poslužitelj preporučeni algoritam šifriranja. Omogućite samo preporučene algoritme na strani poslužitelja, a onemogućite zastarjele.

Prenošenje upotrebom sigurnog FTP-a

Datoteke možete prenijeti sa šifriranjem koristeći se FTPS-om u eksplicitnom načinu rada (FTPES) radi povezivanja s odredišnim poslužiteljem datoteka.
Za siguran prijenos putem FTP-a, postavite [Using Secure Protocol] na [On] u postavkama odredišnog poslužitelja datoteka i uvezite certifikat.

Reference

- 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 (uključuje ažuriranja od 10.6.2016.).

Certifikat

Zapišite certifikat kojim se koristi FTPES (FTPS) funkcija u korijenski direktorij memorijske kartice. Postavite naziv datoteke kako slijedi.
certification.pem (PEM format)
Maksimalna veličina certifikata koja se može učitati je 1 MB po certifikatu.

TP1002274579